

1-525 U.S. PTO
09/27/97
03/26/99

PATENT OFFICE
JAPANESE GOVERNMENT

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application: November 5, 1998

Application Number : P10-315172

Applicant(s) : Nippon Telegraph & Telephone Corporation

February 5, 1999

Commissioner,
Patent Office Takeshi ISAYAMA

Number of Certificate: H 11-3003899

09/27/99
11-90

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1998年11月 5日

出 願 番 号
Application Number:

平成10年特許願第315172号

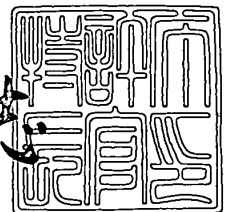
出 願 人
Applicant (s):

日本電信電話株式会社

1999年 2月 5日

特許庁長官
Commissioner,
Patent Office

伴 佐 山 建 志



出証番号 出証特平11-3003899

【書類名】 特許願

【整理番号】 NTTH106186

【提出日】 平成10年11月 5日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/28

【発明の名称】 接続制御方法および通信網と接続制御プログラムおよび
データ構造を記録した記録媒体

【請求項の数】 64

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株
 式会社内

 【氏名】 久田 裕介

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株
 式会社内

 【氏名】 小野 論

【発明者】

 【住所又は居所】 東京都新宿区西新宿三丁目19番2号 日本電信電話株
 式会社内

 【氏名】 市川 晴久

【特許出願人】

 【識別番号】 000004226

 【氏名又は名称】 日本電信電話株式会社

 【代表者】 宮津 純一郎

【代理人】

 【識別番号】 100083806

 【弁理士】

 【氏名又は名称】 三好 秀和

 【電話番号】 03-3504-3075

【選任した代理人】

【識別番号】 100068342

【弁理士】

【氏名又は名称】 三好 保男

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第 79837号

【出願日】 平成10年 3月26日

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第171930号

【出願日】 平成10年 6月18日

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第224861号

【出願日】 平成10年 8月 7日

【手数料の表示】

【予納台帳番号】 001982

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9701396

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体

【特許請求の範囲】

【請求項1】 通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、

第1の機関がユーザの特性を識別する第1の機関の付与情報をユーザに付与し、

第2の機関が前記第1の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、

第3の機関がアクセス権を示す個別化アクセスチケットを発行し、

第4の機関が発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うこと

を特徴とする接続制御方法。

【請求項2】 前記第1の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む1対1個別化アクセスチケットであり、

第4の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項1記載の接続制御方法。

【請求項3】 前記第1の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別

子と1個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含む1対N個別化アクセスチケットであり、

第4の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項1記載の接続制御方法。

【請求項4】 前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストにそのチケットを登録している場合は、第4の機関は当該接続要求を拒否することを特徴とする請求項1または2または3記載の接続制御方法。

【請求項5】 アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、

前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御方法。

【請求項6】 前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項5記載の接続制御方法。

【請求項7】 前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、

第4の機関が発信者からの接続要求に対して、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに

対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項5記載の接続制御方法。

【請求項8】 前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項5記載の接続制御方法。

【請求項9】 個別化アクセスチケット変更権(Enabler)により第3の機関において所有者を変更するときの接続制御方法であって、

第1の個別化アクセスチケットの所有者役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1の役割識別子により新たな所有者役割識別子を変更し、第3の個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項10】 個別化アクセスチケット変更権(Enabler)により第3の機関において会員を追加するときの接続制御方法であって、

所有者が同一である複数の第4の個別化アクセスチケットの所有者役割識別子をそれぞれ第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第3の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記すべての第4の個別化アクセスチケットのすべての会員役割識別子から構成される第5の個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項11】 個別化アクセスチケット変更権(Enabler)により第3の機関において会員を分割するときの接続制御方法であって、

第6の個別化アクセスチケットの所有者役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第4の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記第6の個別化アクセスチケットの一部の会員役割識別子から構成される第7の個別化アクセスチケットを複

数作成することを特徴とする接続制御方法。

【請求項 12】 個別化アクセスチケット変更権(Enabler)により第3の機関において個別化アクセスチケットを新規生成するときの接続制御方法であって、

新規生成する個別化アクセスチケットの所有者役割識別子とする役割識別子と、会員役割識別子とするすべての第5の役割識別子について、それぞれの役割識別子の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第4の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成することを特徴とする接続制御方法。

【請求項 13】 通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、

ユーザの特性を識別する付与情報をユーザに付与する第1の機関と、

前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第2の機関と、

アクセス権を示す個別化アクセスチケットを発行する第3の機関と、

発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第4の機関と

を有することを特徴とする通信網。

【請求項 14】 前記第1の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

前記第4の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換

することで接続制御を行う手段を有することを特徴とする請求項13記載の通信網。

【請求項15】 前記第1の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別子と1個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、

第4の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項13記載の通信網。

【請求項16】 前記第4の機関は、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項13または14または15記載の通信網。

【請求項17】 アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、

前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項18】 前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、

個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化

アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項17記載の接続制御プログラムを記録した記録媒体。

【請求項19】 前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、

第4の機関が発信者からの接続要求を、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項17記載の接続制御プログラムを記録した記録媒体。

【請求項20】 前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項17記載の接続制御プログラムを記録した記録媒体。

【請求項21】 個別化アクセスチケット変更権(Enabler)により第3の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、

第1の個別化アクセスチケットの発信者役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1の役割識別子により新たに発信者役割識別子を変更し、第3の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項22】 個別化アクセスチケット変更権(Enabler)により第3の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、

第4の個別化アクセスチケットの発信者役割識別子を第3の個別化アクセスチ

ケット変更権(Enabler)と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler)、1個以上の第2の役割識別子により1個以上の新たな着信者役割識別子に追加し、第5の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項23】 個別化アクセスチケット変更権(Enabler)により第3の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、

第6の個別化アクセスチケットの発信者役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3の役割識別子により1個以上の着信者役割識別子を削除し、第7の個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項24】 個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケットは、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第3の機関の秘密鍵による署名から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項25】 個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケットは、発信者Index、所有者Index、移転制御情報、発信者役割識別子、1個以上の着信者役割識別子、および有効期限情報から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人

情報、および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項26】 個別化アクセスチケット変更権(Enabler)を記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケット変更権(Enabler)は、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第1の機関の秘密鍵による署名から構成され、

役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項27】 個別化アクセスチケット(PAT)の新規生成および既存の個別化アクセスチケット(PAT)の内容変更を行うために、Null-AID(AID_{Null})および該Null-AIDのEnabler(Enabler of Null-AIDまたはEnabler of AID_{Null})を使用し、該Null-AIDを含む演算は、

(a) 個別化アクセスチケット(PAT)に対する新規生成(MakePAT)、マージ(MergePAT)、分割(SplitPAT)、変更(TransPAT)からなる演算規則に従い、

(b) Null-AIDにのみ適用可能な規則として、

i. Null-AIDは、すべてのユーザに既知であり、

ii. Enabler of Null-AIDは、すべてのユーザに既知である

ことを特徴とする接続制御方法。

【請求項28】 前記Null-AIDは、個別化アクセスチケット（PAT）の所有者AIDとしてのみ使用可能であり、

【数1】

$PAT < AID_{Null} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$
は許可することを特徴とする請求項27記載の接続制御方法。

【請求項29】 God-AID（ AID_{God} ）を用いて、個別化アクセスチケット（PAT）に読取専用属性を設定し、該God-AIDに関する演算は

- (a) God-AIDは、すべてのユーザに既知であり、
- (b) God-AIDに関する演算は、

【数2】

- i. AID所有者が AID_{Null} でも AID_{God} でもない場合：

$PAT < AID_{所有者} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$
+ Enabler of $AID_{所有者}$
→ $PAT < AID_{God} | AID_{所有者}, AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$

- ii. AID所有者が AID_{Null} の場合：

$PAT < AID_{Null} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$
+ Enabler of AID_{Null}
→ $PAT < AID_{God} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$

である場合のいずれかのみ許可されることを特徴とする接続制御方法。

【請求項30】 個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Null-AIDは、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項31】 個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Enabler of Null-AIDは、Enablerであることを表す文字列、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項32】 個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

God-AIDは、God-AIDであることを表す文字列および前記God-AIDであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項33】 通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、

第1の機関がユーザの特性を識別する第1の機関の付与情報をユーザに付与し

第2の機関が前記第1の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、

第3の機関がアクセス権を示すリンク指定型個別化アクセスチケットを発行し

第4の機関が発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うこと

を特徴とする接続制御方法。

【請求項34】 前記第1の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者役割識別子のリンク情報、着信者役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型1対1個別化アクセスチケット

であり、

第4の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型1対1個別化アクセスチケット、および前記リンク指定型1対1個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子のリンク情報がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項33記載の接続制御方法。

【請求項35】 前記第1の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と1個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、

第4の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型1対N個別化アクセスチケット、および前記リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを特徴とする請求項33記載の接続制御方法。

【請求項36】 前記リンク指定型個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストにそのチケットを登録している場合は、第4の機関は当該接続要求を拒否することを特徴と

する請求項33または34または35記載の接続制御方法。

【請求項37】 アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、

前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御方法。

【請求項38】 前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型1対1個別化アクセスチケットであり、

前記リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項37記載の接続制御方法。

【請求項39】 前記個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、

第4の機関が発信者からの接続要求に対して、発信者リンク情報付き役割識別子、1個以上の着信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項37記載の接続制御方法。

【請求項40】 前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特

徴とする請求項 37 記載の接続制御方法。

【請求項 41】 個別化アクセスチケット変更権(Enabler) により第 3 の機関において所有者を変更する方法であって、

第 1 のリンク指定型個別化アクセスチケットのリンク情報で特定される所有者リンク情報付き役割識別子を第 1 の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第 2 の個別化アクセスチケット変更権(Enabler) および第 1 のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第 3 のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項 42】 個別化アクセスチケット変更権(Enabler) により第 3 の機関において会員を追加する方法であって、

所有者が同一である複数の第 4 のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子をそれぞれ第 3 の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、前記第 3 の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記すべての第 4 のリンク指定型個別化アクセスチケットのすべての会員リンク情報付き役割識別子から構成される第 5 のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御方法。

【請求項 43】 個別化アクセスチケット変更権(Enabler) により第 3 の機関において会員を分割するときの接続制御方法であって、

第 6 のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第 4 の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、第 4 の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記第 6 のリンク指定型個別化アクセスチケットの一部の会員リンク情報付き役割識別子から構成される第 7 のリンク指定型個別化アクセスチケットを複数作成することを特徴とする接続制御方法。

【請求項 44】 個別化アクセスチケット変更権(Enabler) により第 3 の機関においてリンク指定型個別化アクセスチケットを新規生成するときの接続制御方法であって、

新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第5のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第4のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成することを特徴とする接続制御方法。

【請求項45】 通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、

ユーザの特性を識別する付与情報をユーザに付与する第1の機関と、

前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第2の機関と、

アクセス権を示すリンク指定型個別化アクセスチケットを発行する第3の機関と、

発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第4の機関と

を有することを特徴とする通信網。

【請求項46】 前記第1の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型1対1個別化アクセスチケットであり、

前記第4の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型1対1個別化アクセスチケット、および前記リンク指定型1対1個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対1個別化アクセスチケットが改竄されていないことを、発信者リンク情報付

き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項45記載の通信網。

【請求項47】 前記第1の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が所有者リンク情報付き役割識別子と1個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、1個以上の会員リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク1対N個別化アクセスチケットであり、

第4の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型1対N個別化アクセスチケット、および前記リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを特徴とする請求項45記載の通信網。

【請求項48】 前記第4の機関は、前記リンク指定型個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを特徴とする請求項45または46または47記載の通信網。

【請求項49】 アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であって、

前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項 50】 前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型 1 対 1 個別化アクセスチケットであり、

リンク指定型 1 対 1 個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型 1 対 1 個別化アクセスチケットに含まれていること、およびリンク情報付き 1 対 1 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項 49 記載の接続制御プログラムを記録した記録媒体。

【請求項 51】 前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1 個以上の着信者リンク情報付き役割識別子のリンク情報、発信者 Index、所有者 Index、移転制御情報、および有効期限情報を含むリンク指定型 1 対 N 個別化アクセスチケットであり、

第 4 の機関が発信者からの接続要求を、発信者リンク情報付き役割識別子、1 個以上の着信者リンク情報付き役割識別子、リンク指定型 1 対 N 個別化アクセスチケット、およびリンク指定型 1 対 N 個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型 1 対 N 個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子が個別化アクセスチケットに含まれていること、およびリンク指定型 1 対 N 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを特徴とする請求項 49 記載の接続制御プログラムを記録した記録媒体。

【請求項 52】 前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを特徴とする請求項 49 記載の接続制御プログラムを記録した記録媒体。

【請求項 53】 個別化アクセスチケット変更権(Enabler) により第3の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、

第1のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第1の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler) および第1のリンク情報付き役割識別子により新たに発信者リンク情報付き役割識別子を変更し、第3のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項 54】 個別化アクセスチケット変更権(Enabler) により第3の期間において会員を追加する方法を実施するプログラムを記録した記録媒体であって、

第4のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第3の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler) 、1個以上の第2のリンク情報付き役割識別子により1個以上の新たな着信者リンク情報付き役割識別子に追加し、第5のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項 55】 個別化アクセスチケット変更権(Enabler) により第3の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、

第6のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第4の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler) 、1個以上の第3のリンク情報付き役割識別子により1個以上の着信者リンク情報付き役割識別子を削除し、第7のリンク指定型個別化アクセスチケットを作成することを特徴とする接続制御プログラムを記録した記録媒体。

【請求項 56】 リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

リンク指定型個別化アクセスチケットは、発信者フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第3の機関の秘密鍵による署名から構成されるリンク指定型1対1個別化アクセスチケットであり、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項57】 リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

リンク指定型個別化アクセスチケットは、発信者Index、所有者Index、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク指定型1対N個別化アクセスチケットであり、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報、および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項58】 個別化アクセスチケット変更権(Enabler)を記録したコンピュータで読み取り可能な記録媒体であって、

個別化アクセスチケット変更権(Enabler)は、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第1の機関の秘密鍵による署名から構成され、

リンク情報付き役割識別子は、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報、および第1の機関の秘密鍵による署名から構成され、

個人識別子は、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、

発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録した記録媒体。

【請求項59】 リンク指定型個別化アクセスチケット（PAT）の新規生成および既存のリンク指定型個別化アクセスチケット（PAT）の内容変更を行うため、Null-AID（AID_{Null}）および該Null-AIDのEnabler（Enabler of Null-AIDまたはEnabler of AID_{Null}）を使用し、該Null-AIDを含む演算は、

(a) リンク指定型個別化アクセスチケット（PAT）に対する新規生成（Make PAT）、マージ（Merge PAT）、分割（Split PAT）、変更（Trans PAT）からなる演算規則に従い、

(b) Null-AIDにのみ適用可能な規則として、

i. Null-AIDは、すべてのユーザに既知であり、

ii. Enabler of Null-AIDは、すべてのユーザに既知である

ことを特徴とする接続制御方法。

【請求項60】 前記Null-AIDは、リンク指定型個別化アクセスチケット（PAT）の所有者AIDとしてのみ使用可能であり、

【数3】

$PAT < AID_{Null} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$
は許可することを特徴とする請求項59記載の接続制御方法。

【請求項61】 God-AID（AID_{God}）を用いて、リンク指定型個別化アクセスチケット（PAT）に読取専用属性を設定し、該God-AIDに関する演算は、

(a) God-AIDは、すべてのユーザに既知であり、

(b) God-AIDに関する演算は、

【数4】

i. AID_{所有者}がAID_{Null}でもAID_{God}でもない場合：

PAT < AID_{所有者} | AID_{会員1} , AID_{会員2} ,
..., AID_{会員N} >

+ Enabler of AID_{所有者}

→ PAT < AID_{God} | AID_{所有者} , AID_{会員1} , AID_{会員2} ,
..., AID_{会員N} >

ii. AID_{所有者}がAID_{Null}の場合：

PAT < AID_{Null} | AID_{会員1} , AID_{会員2} ,
..., AID_{会員N} >

+ Enabler of AID_{Null}

→ PAT < AID_{God} | AID_{会員1} , AID_{会員2} ,
..., AID_{会員N} >

である場合のいずれかのみ許可されることを特徴とする接続制御方法。

【請求項62】 リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Null-AIDは、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項63】 リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

Enabler of Null-AIDは、Enablerであることを表す文字列、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録した記録媒体。

【請求項64】 リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、

God-AIDは、God-AIDであることを表す文字列および前記God-AIDであることを表す文字列に対して認証局の署名を施したものであること

を特徴とするデータ構造を記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、通信網において着信者の通信網における識別子を隠蔽しつつ、通信網における識別子を隠蔽した他のユーザからの通信の接続を制御する接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体に関する。

【0002】

【従来の技術】

近年、電話やコンピュータネットワークを用いた個人攻撃、例えば嫌がらせ、名誉毀損等が深刻な社会問題になっている。このような個人攻撃は通信網を介して氏名、性別、年齢、電話番号、電子メールアドレスといったプライバシー情報が第三者に漏洩するために発生するものである。具体的には、第三者による盗聴、偽装等の盗難、第三者による意図的な収集（アンケート）、発信者の間違い電話等の端末操作ミス、発信者によるやむを得ない公開（情報誌、電子掲示板、ホームページ等）がある。

【0003】

現在、盗難対策には認証、暗号化があり、間違い電話対策には端末の電話帳機能がある。また、第三者によるアンケート等の意図的な収集および発信者によるやむを得ない公開に対しては、いくつかの対策が実施されているが、いずれも漏洩を完全に防止することはできない。

【0004】

求人（仲間募集）や売買のように他のユーザと個人的に連絡を取る必要があるユーザは、最低限、氏名と連絡先を情報誌、電子掲示板、またはホームページに掲載しなければならない。また、性別、年齢といったプライバシー情報を公開しなければならない場合もある。ところが、これらのメディアを閲覧するのは善意のユーザだけではない。個人攻撃を仕掛けようと企むユーザも閲覧する可能性は決して小さくない。そこで、情報を公開したユーザを何らかの手段で個人攻撃か

ら保護することが必要になる。

【0005】

このとき、そのユーザの取り得る戦略は2種類ある。ひとつは情報を限定公開する戦略で、具体的にはニックネームがある。もうひとつは接続相手を着信側で限定する戦略で、具体的には二重番号登録、発信者番号通知、着信拒否、匿名電子メール(Anonymous Mails)がある。

【0006】

インターネットやパソコン通信の電子掲示板システムではニックネーム(ハンドルネーム)による発信が可能のため、実名を隠蔽することができる。しかしながら、善意のユーザにはすべてのプライバシー情報を公開するけれども、悪意のユーザには公開しないといったような制御はできないし、発信者の電子メールアドレスも隠蔽できない。このため、第三者から攻撃される恐れがある。

【0007】

二重番号では、図27に示すように、回線に複数の電話番号を割り当て、そのうちの一部の番号への呼をすべて自動的に切断するため、個人攻撃を被る恐れはない。その代わり、着呼可能な番号を知る者には厳重に守秘義務が課される。

【0008】

また、発信者番号通知は、図28に示すように、発信者電話番号を着信側端末に通知するものであり、アナログ公衆網、ISDN、デジタル携帯網で提供されているが、番号非通知の場合には、着信端末にも何も表示されない。

【0009】

一方、着信拒否は、図29に示すように、呼を自動的に切断する機能であり、アナログ公衆網、ISDN、デジタル携帯網で提供されている。仕様は網によって異なる。アナログ公衆網とISDNでは、着信側回線あるいは端末で指定した発信者番号の呼以外は接続しない。逆に、デジタル携帯網では、着信側端末で設定した発信者番号の呼を切断する。

【0010】

一般に、発信者番号通知と着信拒否は組み合わせて利用される。ところが、両者を組み合わせると、発信者と着信者のいずれか一方しか保護できなくなる。ア

ナログ公衆網やISDNでは番号非通知の呼を切断するため、番号漏洩を防止できなくなる。仕様を逆手にとると、個人情報の収集手段として利用できるからである。一方、デジタル携帯網では番号非通知の呼を切断しないため、着信者を個人攻撃から保護できなくなる。

【0011】

匿名電子メールでは、図30に示すように、発信者メールアドレスをリメーラ(remailer)機能を持つメールサーバのメールアドレスに書き換えて送信先に転送する。このように、発信者メールアドレスを隠蔽するため、発信者メールアドレスの漏洩を防ぐことができる。その一方で、匿名による攻撃が可能になるため、着信者が第三者から攻撃される危険性はより高くなる。

【0012】

これを防ぐために、着信者から要求があった場合には、リメーラはその着信者宛の匿名メールの配信を中止する。ところが、この機能を用いると番号漏洩を防ぐことはできなくなる。着信拒否同様、個人情報の収集手段として利用できるからである。

【0013】

【発明が解決しようとする課題】

上述したように、従来のニックネーム、二重番号登録、発信者番号通知、着信拒否、匿名電子メール等の方法では、それぞれ発信者の電子メールアドレスを隠蔽できず、第三者から攻撃されたり、着呼可能番号を知る者に厳重な守秘義務が課せられたり、番号非通知の呼を切断しない場合もあり、着信者を個人攻撃から保護できなかったり、匿名による攻撃が可能となり、着信者が第三者から攻撃される危険性が高くなるというような種々の問題がある。

【0014】

本発明は、上記に鑑みてなされたもので、その目的とするところは、第三者による意図的な収集およびユーザによるやむを得ない公開に対して匿名性とセキュリティを確保すべく発信者および着信者の匿名性を保持しつつ発信者からの通信の接続を可能とし、着信者が匿名性を悪用した発信者による攻撃にさらされた場合には、その攻撃による着信者への被害を食い止めることを可能とする接続制御

方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体を提供することにある。

【0015】

【課題を解決するための手段】

上記目的を達成するため、請求項1記載の本発明は、通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、第1の機関がユーザの特性を識別する第1の機関の付与情報をユーザに付与し、第2の機関が前記第1の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、第3の機関がアクセス権を示す個別化アクセスチケットを発行し、第4の機関が発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うことを要旨とする。

【0016】

請求項1記載の本発明にあつては、第1の機関の付与情報をユーザに付与し、第1の機関の付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【0017】

また、請求項2記載の本発明は、請求項1記載の発明において、前記第1の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含む1対1個別化アクセスチケットであり、第4の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検

証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【0018】

請求項2記載の本発明にあっては、第1の機関の付与情報は役割識別子であり、発信者の指定情報は発信者役割識別子と着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含む1対1個別化アクセスチケットであり、役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0019】

更に、請求項3記載の本発明は、請求項1記載の発明において、前記第1の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別子と1個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含む1対N個別化アクセスチケットであり、第4の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【0020】

請求項3記載の本発明にあっては、第1の機関の付与情報は発信者役割識別子

と個別化アクセスチケット変更権(Enabler)であり、発信者の指定情報は発信者役割識別子と1個以上の着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含む1対N個別化アクセスチケットであり、発信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0021】

請求項4記載の本発明は、請求項1または2または3記載の発明において、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストにそのチケットを登録している場合は、第4の機関は当該接続要求を拒否することを要旨とする。

【0022】

請求項4記載の本発明にあつては、個別化アクセスチケットに関する認証結果が正しくても、着信者の個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【0023】

また、請求項5記載の本発明は、アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法において、前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを要旨とする。

【0024】

請求項5記載の本発明にあつては、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する。

【0025】

更に、請求項6記載の本発明は、請求項5記載の発明において、前記個別化ア

クセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【0026】

請求項6記載の本発明にあっては、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う。

【0027】

請求項7記載の本発明は、請求項5記載の発明において、前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、第4の機関が発信者からの接続要求に対して、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【0028】

請求項7記載の本発明にあっては、個別化アクセスチケットが発信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3

要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う。

【0029】

また、請求項 8 記載の本発明は、請求項 5 記載の発明において、前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを要旨とする。

【0030】

請求項 8 記載の本発明にあつては、検証結果が正しくても個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する。

【0031】

更に、請求項 9 記載の本発明は、個別化アクセスチケット変更権(Enabler)により第 3 の機関において所有者を変更するときの接続制御方法であつて、第 1 の個別化アクセスチケットの所有者役割識別子を第 1 の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第 2 の個別化アクセスチケット変更権(Enabler)および第 1 の役割識別子により新たな所有者役割識別子を変更し、第 3 の個別化アクセスチケットを作成することを要旨とする。

【0032】

請求項 9 記載の本発明にあつては、第 1 の個別化アクセスチケットの所有者役割識別子を第 1 の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第 2 の個別化アクセスチケット変更権(Enabler)および第 1 の役割識別子により新たな所有者役割識別子を変更し、第 3 の個別化アクセスチケットを作成する。

【0033】

請求項 10 記載の本発明は、個別化アクセスチケット変更権(Enabler)により第 3 の機関において会員を追加するときの接続制御方法であつて、所有者が同一である複数の第 4 の個別化アクセスチケットの所有者役割識別子をそれぞれ第 3 の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第 3 の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記すべての第 4 の個別化アクセスチケットのすべての会員役割識別子から構成される第 5

の個別化アクセスチケットを作成することを要旨とする。

【0034】

請求項10記載の本発明にあっては、第4の個別化アクセスチケットの所有者役割識別子を第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler)、1個以上の第2の役割識別子により1個以上の新たな会員役割識別子に追加すなわち連結し、第5の個別化アクセスチケットを作成する。

【0035】

尚、同一所有者役割識別子の複数個別化アクセスチケットをマージする演算は【数5】

$$\begin{aligned}
 & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員am} > \\
 & + PAT < AID_{所有者} | AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bn} > \\
 & + \text{Enabler of } AID_{所有者} \\
 & \longrightarrow \\
 & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員am}, \\
 & \quad AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bn} >
 \end{aligned}$$

である。

【0036】

また、請求項11記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を分割するときの接続制御方法であって、第6の個別化アクセスチケットの所有者役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第4の個別化アクセスチケット変更権を用いて、前記所有者役割識別子と前記第6の個別化アクセスチケットの一部の会員役割識別子から構成される第7の個別化アクセスチケットを複数作成することを要旨とする。

【0037】

請求項11記載の本発明にあっては、第6の個別化アクセスチケットの所有者

役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3の役割識別子により1個以上の会員役割識別子を分割、具体的には例えば削除し、第7の個別化アクセスチケットを作成する。

【0038】

尚、個別化アクセスチケットを同一所有者役割識別子の複数個別化アクセスチケットに分割する演算は、

【数6】

$$\begin{aligned}
 & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員aN} \\
 & \quad AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} > \\
 & + \text{Enabler of } AID_{所有者} \\
 \longrightarrow & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員aN} > \\
 & + PAT < AID_{所有者} | AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} >
 \end{aligned}$$

である。

【0039】

また、請求項12記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において個別化アクセスチケットを新規生成するときの接続制御方法であって、新規生成する個別化アクセスチケットの所有者役割識別子とする役割識別子と、会員役割識別子とするすべての第5の役割識別子について、それぞれの役割識別子の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第4の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成することを要旨とする。

【0040】

請求項12記載の本発明にあつては、これから新規生成する個別化アクセスチケットの第5の所有者役割識別子とする第4の役割識別子と、会員役割識別子とするすべての第5の役割識別子について、それぞれの役割識別子の個別化アクセ

スチケット変更権(Enabler)で照合し、照合結果が、正しい場合に、第4の役割識別子を所有者役割識別子とする個別化アクセスチケットを新規生成する。

【0041】

更に、請求項13記載の本発明は、通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であって、ユーザの特性を識別する付与情報をユーザに付与する第1の機関と、前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第2の機関と、アクセス権を示す個別化アクセスチケットを発行する第3の機関と、発信者からの発信要求に対して前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第4の機関とを有することを要旨とする。

【0042】

請求項13記載の本発明にあっては、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【0043】

請求項14記載の本発明は、請求項13記載の発明において、前記第1の機関の付与情報が役割識別子であり、前記発信者の指定情報が発信者役割識別子と着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、および有効期限を含み、前記第4の機関は発信者からの接続要求を、前記役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【0044】

請求項 14 記載の本発明にあつては、第 1 の機関の付与情報は役割識別子であり、発信者の指定情報は発信者役割識別子と着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0045】

また、請求項 15 記載の本発明は、請求項 13 記載の発明において、前記第 1 の機関の付与情報が発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者役割識別子と 1 個以上の着信者役割識別子であり、前記個別化アクセスチケットが発信者役割識別子、1 個以上の着信者役割識別子、発信者 Index、所有者 Index、移転制御情報、および有効期限情報を含み、第 4 の機関は発信者からの接続要求を、前記発信者役割識別子、前記個別化アクセスチケット、および前記個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、第 4 の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【0046】

請求項 15 記載の本発明にあつては、第 1 の機関の付与情報は発信者役割識別子と個別化アクセスチケット変更権(Enabler)であり、発信者の指定情報は発信者役割識別子と 1 個以上の着信者役割識別子であり、個別化アクセスチケットは発信者役割識別子、1 個以上の着信者役割識別子、発信者 Index、所有者 Index、移転制御情報、および有効期限情報を含み、発信者役割識別子、個別化アクセ

スチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0047】

更に、請求項16記載の本発明は、請求項13または14または15記載の発明において、前記第4の機関が、前記個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【0048】

請求項16記載の本発明にあつては、個別化アクセスチケットに関する認証結果が正しくても、着信者が着信拒否リストに該個別化アクセスチケットを登録している場合は、当該接続要求を拒否する。

【0049】

請求項17記載の本発明は、アクセス権を示す情報である個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であつて、前記個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録することを要旨とする。

【0050】

請求項17記載の本発明にあつては、個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0051】

また、請求項18記載の本発明は、請求項17記載の発明において、前記個別化アクセスチケットが発信者役割識別子、着信者役割識別子、発信者フラグ、移

転制御フラグ、および有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【0052】

請求項18記載の本発明にあっては、個別化アクセスチケットは発信者役割識別子、着信者役割識別子、発信者フラグ、移転制御フラグ、有効期限を含み、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0053】

更に、請求項19記載の本発明は、請求項17記載の発明において、前記個別化アクセスチケットが発信者役割識別子、1個以上の着信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、第4の機関が発信者からの接続要求を、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、および個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセスチケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【0054】

請求項19記載の本発明にあっては、個別化アクセスチケットが発信者役割識別子、発信者Index、所有者Index、移転制御情報、および有効期限情報を含み、発信者役割識別子、1個以上の着信者役割識別子、個別化アクセスチケット、個別化アクセスチケットに対する電子署名の持つ情報を用いて、個別化アクセス

チケットが改竄されていないこと、発信者役割識別子が個別化アクセスチケットに含まれていること、および個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0055】

請求項20記載の本発明は、請求項17記載の発明において、前記検証結果が正しくても、個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録することを要旨とする。

【0056】

請求項20記載の本発明にあつては、検証結果が正しくても個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0057】

また、請求項21記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であつて、第1の個別化アクセスチケットの発信者役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1の役割識別子により新たに発信者役割識別子を変更し、第3の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0058】

請求項21記載の本発明にあつては、第1の個別化アクセスチケットの発信者役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1の役割識別子により新たな発信者役割識別子を変更し、第3の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、そ

の流通性を高めることができる。

【0059】

更に、請求項22記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、第4の個別化アクセスチケットの発信者役割識別子を第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler)、1個以上の第2の役割識別子により1個以上の新たな着信者役割識別子に追加し、第5の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0060】

請求項22記載の本発明にあつては、第4の個別化アクセスチケットの発信者役割識別子を第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler)、1個以上の第2の役割識別子により1個以上の新たな着信者役割識別子に追加し、第5の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0061】

請求項23記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、第6の個別化アクセスチケットの発信者役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3の役割識別子により1個以上の着信者役割識別子を削除し、第7の個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0062】

請求項23記載の本発明にあつては、第6の個別化アクセスチケットの発信者役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3の役割識別子により1個以上の着信者役割識別子を削除し、第7の個別化

アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0063】

また、請求項24記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケットが、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第3の機関の秘密鍵による署名から構成され、役割識別子が、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、および第1の機関の秘密鍵による署名から構成され、個人識別子が、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0064】

請求項24記載の本発明にあつては、発信者フラグ、移転制御フラグ、発信者役割識別子、着信者役割識別子、有効期限、および第3の機関の秘密鍵による署名から構成される個別化アクセスチケットを発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0065】

更に、請求項25記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、個別化アクセスチケットが、発信者Index、所有者Index、移転制御情報、発信者役割識別子、1個以上の着信者役割識別子、および有効期限情報から構成され、役割識別子が、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、および第1の機関の秘密鍵による署名から構成され、個人識別子が、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0066】

請求項 25 記載の本発明にあつては、発信者 Index、所有者 Index、移転制御情報、発信者役割識別子、1 個以上の着信者役割識別子、および有効期限情報から構成される個別化アクセスチケットを発信者と着信者の 1 対 N 対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0067】

請求項 26 記載の本発明は、個別化アクセスチケット変更権(Enabler)を記録したコンピュータで読み取り可能な記録媒体であつて、個別化アクセスチケット変更権(Enabler)が、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第 1 の機関の秘密鍵による署名から構成され、役割識別子が、個人識別子、暗号化された位置情報、第 4 の機関のホスト個人情報、および第 1 の機関の秘密鍵による署名から構成され、個人識別子が、第 1 の機関が一意に付与した文字列、および第 1 の機関の秘密鍵による署名から構成され、発信者と着信者の 1 対 N 対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0068】

請求項 26 記載の本発明にあつては、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第 1 の機関の秘密鍵による署名から構成される個別化アクセスチケット変更権(Enabler)を発信者と着信者の 1 対 N 対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0069】

請求項 27 記載の本発明は、個別化アクセスチケット(PAT)の新規生成および既存の個別化アクセスチケット(PAT)の内容変更を行うために、Null-AID(AID_{Null})および該Null-AIDのEnabler(Enabler of Null-AIDまたはEnabler of AID_{Null})を使用し、該Null-AIDを含む演算が、

(a) 個別化アクセスチケット (PAT) に対する新規生成 (MakePAT)、マージ (MergePAT)、分割 (SplitPAT)、変更 (TransPAT) からなる演算規則に従い、

(b) Null-AIDにのみ適用可能な規則として、

i. Null-AIDは、すべてのユーザに既知であり、

ii. Enabler of Null-AIDは、すべてのユーザに既知である

ことを要旨とする。

【0070】

請求項27記載の本発明にあつては、個別化アクセスチケット (PAT) の新規生成および既存の個別化アクセスチケット (PAT) の内容変更を行うために、Null-AID (AID_{Null}) および該Null-AIDの Enabler (Enabler of Null-AIDまたは Enabler of AID_{Null}) を使用するため、会員AIDおよび Enabler of 会員AIDを所有者AIDに渡さなくても新規生成 (MakePAT) およびマージ (MergePAT) を行うことができる。

【0071】

また、請求項28記載の本発明は、請求項27記載の発明において、前記Null-AIDが、個別化アクセスチケット (PAT) の所有者AIDとしてのみ使用可能であり、

【数7】

$PAT < AID_{Null} | AID_{\text{会員1}}, AID_{\text{会員2}}, \dots, AID_{\text{会員N}} >$
は許可することを要旨とする。

【0072】

請求項28記載の本発明にあつては、Null-AIDは個別化アクセスチケット (PAT) の所有者AIDとしてのみ使用可能であり、

【数8】

$PAT < AID_{Null} | AID_{\text{会員1}}, AID_{\text{会員2}}, \dots, AID_{\text{会員N}} >$
は許可するため、 $PAT < AID_{\text{所有者}} | AID_{\text{会員}} >$ の所有者がAID_{会員}の Enabler を知らない場合には、このPATから $PAT < AID_{Null} | AID_{\text{会員}} >$ を作成することはできない。

【0073】

更に、請求項29記載の本発明は、God-AID (AID_{God}) を用いて、個別化アクセスチケット (PAT) に読取専用属性を設定し、該God-AID に関する演算が、

- (a) God-AID は、すべてのユーザに既知であり、
- (b) God-AID に関する演算が、

【数9】

- i. AID_{所有者}がAID_{Null}でもAID_{God}でもない場合：

$$PAT < AID_{所有者} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$$

$$+ \text{Enabler of } AID_{所有者}$$

$$\rightarrow PAT < AID_{God} | AID_{所有者}, AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$$
- ii. AID_{所有者}がAID_{Null}の場合：

$$PAT < AID_{Null} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$$

$$+ \text{Enabler of } AID_{Null}$$

$$\rightarrow PAT < AID_{God} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$$

である場合のいずれかのみ許可されることを要旨とする。

【0074】

請求項29記載の本発明にあっては、God-AID (AID_{God}) を用いて、個別化アクセスチケット (PAT) に読取専用属性を設定するため、グループ通信において参加者を固定することができる。

【0075】

更に、請求項30記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Null-AIDが、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0076】

請求項30記載の本発明にあつては、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したものであるデータ構造のNull-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0077】

請求項31記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であつて、Enabler of Null-AIDは、Enablerであることを表す文字列、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0078】

請求項31記載の本発明にあつては、Enablerであることを表す文字列、Null-AIDの実体、およびEnablerであることを表す文字列とNull-AIDの実体を連結した文字列に対して認証局の署名を施したものであるデータ構造のEnabler of Null-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0079】

また、請求項32記載の本発明は、個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であつて、God-AIDが、God-AIDであることを表す文字列および前記God-AIDであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0080】

請求項32記載の本発明にあつては、God-AIDであることを表す文字列およびGod-AIDであることを表す文字列に対して認証局の署名を施したものであるデータ構造のGod-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0081】

更に、請求項 33 記載の本発明は、通信網におけるユーザ個人を隠蔽した通信の接続制御方法であって、第 1 の機関がユーザの特性を識別する第 1 の機関の付与情報をユーザに付与し、第 2 の機関が前記第 1 の機関の付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定し、第 3 の機関がアクセス権を示すリンク指定型個別化アクセスチケットを発行し、第 4 の機関が発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うことを要旨とする。

【0082】

請求項 33 記載の本発明にあつては、第 1 の機関の付与情報をユーザに付与し、第 1 の機関の付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示すリンク指定型個別化アクセスチケットを発行し、発信者からの発信要求に対してリンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【0083】

請求項 34 記載の本発明は、請求項 33 記載の発明において、前記第 1 の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが発信者役割識別子のリンク情報、着信者役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型 1 対 1 個別化アクセスチケットであり、第 4 の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型 1 対 1 個別化アクセスチケット、および前記リンク指定型 1 対 1 個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型 1 対 1 個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子のリンク情報がリンク指定型 1 対 1 個別化アクセスチケットに含まれていること、およびリンク指定型 1 対 1 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、

検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【0084】

請求項34記載の本発明にあっては、第1の機関の付与情報はリンク情報付き役割識別子であり、発信者の指定情報は発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型1対1個別化アクセスチケットであり、リンク情報付き役割識別子、リンク指定型1対1個別化アクセスチケット、リンク指定型1対1個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0085】

また、請求項35記載の本発明は、請求項33記載の発明において、前記第1の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler)であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と1個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、第4の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型1対N個別化アクセスチケット、および前記リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに

含まれていること、およびリンク指定型 1 対 N 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、第 4 の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行うことを要旨とする。

【0086】

請求項 35 記載の本発明にあっては、第 1 の機関の付与情報は所有者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler)であり、発信者の指定情報は発信者リンク情報付き役割識別子と 1 個以上の着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは所有者リンク情報付き役割識別子のリンク情報、1 個以上の着信者リンク情報付き役割識別子のリンク情報、発信者 Index、所有者 Index、移転制御情報、および有効期限情報を含むリンク指定型 1 対 N 個別化アクセスチケットであり、発信者リンク情報付き役割識別子、リンク指定型 1 対 N 個別化アクセスチケット、リンク指定型 1 対 N 個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型 1 対 N 個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型 1 対 N 個別化アクセスチケットに含まれていること、およびリンク指定型 1 対 N 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0087】

更に、請求項 36 記載の本発明は、請求項 33 または 34 または 35 記載の発明において、前記リンク指定型個別化アクセスチケットに関する第 4 の機関の認証結果が正しくても、着信者が第 4 の機関の着信拒否リストにそのチケットを登録している場合は、第 4 の機関は当該接続要求を拒否することを要旨とする。

【0088】

請求項 36 記載の本発明にあっては、リンク指定型 1 対 N 個別化アクセスチケットに関する認証結果が正しくても、着信者のリンク指定型 1 対 N 個別化アクセスチケットが着信拒否リストに登録している場合は、接続要求を拒否する。

【0089】

請求項37記載の本発明は、アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する接続制御方法であって、前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続することを要旨とする。

【0090】

請求項37記載の本発明にあつては、リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する。

【0091】

また、請求項38記載の本発明は、請求項37記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型1対1個別化アクセスチケットであり、前記リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【0092】

請求項38記載の本発明にあつては、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型1対1であり、リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う。

【0093】

更に、請求項39記載の本発明は、請求項37記載の発明において、前記個別

化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、第4の機関が発信者からの接続要求に対して、発信者リンク情報付き役割識別子、1個以上の着信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行うことを要旨とする。

【0094】

請求項39記載の本発明にあっては、リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、所有者リンク情報付き役割識別子、1個以上の着信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う。

【0095】

請求項40記載の本発明は、請求項37記載の発明において、前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否することを要旨とする。

【0096】

請求項40記載の本発明にあつては、検証結果が正しくてもリンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する。

【0097】

また、請求項41記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において所有者を変更する方法であつて、第1のリンク指定型個別化アクセスチケットのリンク情報で特定される所有者リンク情報付き役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第3のリンク指定型個別化アクセスチケットを作成することを要旨とする。

【0098】

請求項41記載の本発明にあつては、第1のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)および第1のリンク情報付き役割識別子により新たな所有者リンク情報付き役割識別子を変更し、第3のリンク指定型個別化アクセスチケットを作成する。

【0099】

更に、請求項42記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を追加する接続制御方法であつて、所有者が同一である複数の第4のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子をそれぞれ第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、前記第3の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記すべての第4のリンク指定型個別化アクセスチケットのすべての会員リンク情報付き役割識別子から構成される第5のリンク指定型個別化アクセスチケットを作成することを要旨とする。

【0100】

請求項42記載の本発明にあっては、第4の個別化アクセスチケットの所有者役割識別子を第3の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler)、1個以上の第2の役割識別子により1個以上の新たな会員役割識別子に追加すなわち連結し、第5の個別化アクセスチケットを作成する。

【0101】

なお、同一所有者役割識別子の複数個個別化アクセスチケットをマージする演算は、

【数10】

$$\begin{aligned} & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員aN} > \\ & + PAT < AID_{所有者} | AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} > \\ & + \text{Enabler of } AID_{所有者} \\ & \longrightarrow \\ & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員aN} \\ & \quad AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} > \end{aligned}$$

である。

【0102】

請求項43記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を分割するときの接続制御方法であって、第6のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、第4の個別化アクセスチケット変更権を用いて、前記所有者リンク情報付き役割識別子と前記第6のリンク指定型個別化アクセスチケットの一部の会員リンク情報付き役割識別子から構成される第7のリンク指定型個別化アクセスチケットを複数作成することを要旨とする。

【0103】

請求項 4 3 記載の本発明にあつては、第 6 のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第 4 の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、1 個以上の第 5 の個別化アクセスチケット変更権(Enabler) 、1 個以上の第 3 のリンク情報付き役割識別子により 1 個以上の会員リンク情報付き役割識別子を分類、具体的には例えば削除し、第 7 のリンク指定型個別化アクセスチケットを作成する。

【0104】

なお、リンク指定型個別化アクセスチケットを同一所有者役割識別子の複数のリンク指定型個別化アクセスチケットに分割する演算は、

【数 1 1】

$$\begin{aligned}
 & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員an} \\
 & \quad AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} > \\
 & + \text{Enabler of } AID_{所有者} \\
 & \longrightarrow \\
 & PAT < AID_{所有者} | AID_{会員a1}, AID_{会員a2}, \dots, AID_{会員an} > \\
 & + PAT < AID_{所有者} | AID_{会員b1}, AID_{会員b2}, \dots, AID_{会員bN} >
 \end{aligned}$$

である。

【0105】

また、請求項 4 4 記載の本発明は、個別化アクセスチケット変更権(Enabler) により第 3 の機関においてリンク指定型個別化アクセスチケットを新規生成するときの接続制御方法であつて、新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第 5 のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第 4 のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成

することを要旨とする。

【0106】

請求項44記載の本発明にあつては、新規生成するリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子とするリンク情報付き役割識別子と、会員リンク情報付き役割識別子とするすべての第5のリンク情報付き役割識別子について、それぞれのリンク情報付き役割識別子の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第4のリンク情報付き役割識別子を所有者リンク情報付き役割識別子とするリンク指定型個別化アクセスチケットを新規生成する。

【0107】

更に、請求項45記載の本発明は、通信網においてユーザ個人を隠蔽した通信を制御可能とする通信網であつて、ユーザの特性を識別する付与情報をユーザに付与する第1の機関と、前記付与情報とユーザに関する情報とを対にし、他のユーザから閲覧可能なように保持し、発信者がユーザ間の対応を示す発信者の指定情報を指定する第2の機関と、アクセス権を示すリンク指定型個別化アクセスチケットを発行する第3の機関と、発信者からの発信要求に対して前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う第4の機関とを有することを要旨とする。

【0108】

請求項45記載の本発明にあつては、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザからの閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示すリンク指定型個別化アクセスチケットを発行し、発信者からの発信要求に対してリンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行う。

【0109】

請求項46記載の本発明は、請求項45記載の発明において、前記第1の機関の付与情報がリンク情報付き役割識別子であり、前記発信者の指定情報が発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、前記リン

ク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型 1 対 1 個別化アクセスチケットであり、前記第 4 の機関は発信者からの接続要求を、前記リンク情報付き役割識別子、前記リンク指定型 1 対 1 個別化アクセスチケット、および前記リンク指定型 1 対 1 個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型 1 対 1 個別化アクセスチケットが改竄されていないことを、発信者リンク情報付き役割識別子がリンク指定型 1 対 1 個別化アクセスチケットに含まれていること、およびリンク指定型 1 対 1 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、第 4 の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【0110】

請求項 46 記載の本発明にあつては、第 1 の機関の付与情報はリンク情報付き役割識別子であり、発信者の指定情報は発信者リンク情報付き役割識別子と着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型 1 対 1 であり、役割リンク情報付き識別子、リンク指定型 1 対 1 個別化アクセスチケット、リンク指定型 1 対 1 個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型 1 対 1 個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型 1 対 1 個別化アクセスチケットに含まれていること、およびリンク指定型 1 対 1 個別化アクセスチケットが有効期限内であることの 3 要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0111】

また、請求項 47 記載の本発明は、請求項 45 記載の発明において、前記第 1 の機関の付与情報が発信者リンク情報付き役割識別子と個別化アクセスチケット

変更権(Enabler)であり、前記発信者の指定情報が所有者リンク情報付き役割識別子と1個以上の着信者リンク情報付き役割識別子であり、前記リンク指定型個別化アクセスチケットが所有者リンク情報付き役割識別子のリンク情報、1個以上の会員リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク1対N個別化アクセスチケットであり、第4の機関は発信者からの接続要求を、前記発信者リンク情報付き役割識別子、前記リンク指定型1対N個別化アクセスチケット、および前記リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、第4の機関が接続している通信網における物理的な接続制御方式に変換することで接続制御を行う手段を有することを要旨とする。

【0112】

請求項47記載の本発明にあつては、第1の機関の付与情報は発信者リンク情報付き役割識別子と個別化アクセスチケット変更権(Enabler)であり、発信者の指定情報は発信者リンク情報付き役割識別子と1個以上の着信者リンク情報付き役割識別子であり、リンク指定型個別化アクセスチケットは所有者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、発信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に、発信者からの接続要求を通信網の物理的な接続制御方式に変換して接続制御を行う。

【0113】

更に、請求項48記載の本発明は、請求項45または46または47記載の発明において、前記第4の機関が、前記リンク指定型個別化アクセスチケットに関する第4の機関の認証結果が正しくても、着信者が第4の機関の着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、第4の機関は当該接続要求を拒否する拒否手段を有することを要旨とする。

【0114】

請求項48記載の本発明にあつては、リンク指定型個別化アクセスチケットに関する認証結果が正しくても、着信者が着信拒否リストに該リンク指定型個別化アクセスチケットを登録している場合は、当該接続要求を拒否する。

【0115】

請求項49記載の本発明は、アクセス権を示す情報であるリンク指定型個別化アクセスチケットを用いて、ユーザ間の通信を制御する方法を実施するプログラムを記録した記録媒体であつて、前記リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録することを要旨とする。

【0116】

請求項49記載の本発明にあつては、リンク指定型個別化アクセスチケットを用いてアクセス権を検証し、検証結果が正しい場合にユーザ間を接続する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0117】

また、請求項50記載の本発明は、請求項49記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、および有効期限を含むリンク指定型1対1個別化アクセスチケットであり、リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク情報付き1対1個別化アクセスチケットが有効期限

内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【0118】

請求項50記載の本発明にあっては、リンク指定型個別化アクセスチケットは発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、発信者フラグ、移転制御フラグ、有効期限を含むリンク指定型1対1個別化アクセスチケットであり、リンク指定型1対1個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対1個別化アクセスチケットに含まれていること、およびリンク指定型1対1個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0119】

更に、請求項51記載の本発明は、請求項49記載の発明において、前記リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N個別化アクセスチケットであり、第4の機関が発信者からの接続要求を、発信者リンク情報付き役割識別子、1個以上の着信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子が個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、ユーザ間の接続を行う接続制御プログラムを記録媒体に記録することを要旨とする。

【0120】

請求項51記載の本発明にあっては、リンク指定型個別化アクセスチケットが発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、発信者Index、所有者Index、移転制御情報、および有効期限情報を含むリンク指定型1対N所有者役割識別子であり、発信者リンク情報付き役割識別子、1個以上の着信者リンク情報付き役割識別子、リンク指定型1対N個別化アクセスチケット、リンク指定型1対N個別化アクセスチケットに対する電子署名の持つ情報を用いて、リンク指定型1対N個別化アクセスチケットが改竄されていないこと、発信者リンク情報付き役割識別子がリンク指定型1対N個別化アクセスチケットに含まれていること、およびリンク指定型1対N個別化アクセスチケットが有効期限内であることの3要件をすべて検証し、検証結果がすべて正しい場合に限り、発信者からの接続要求に対してユーザ間の接続を行う接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0121】

請求項52記載の本発明は、請求項49記載の発明において、前記検証結果が正しくても、リンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録することを要旨とする。

【0122】

請求項52記載の本発明にあっては、検証結果が正しくてもリンク指定型個別化アクセスチケットが着信拒否リストにある場合、ユーザ間の接続要求を拒否する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0123】

また、請求項53記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において所有者を変更する方法を実施するプログラムを記録した記録媒体であって、第1のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合

し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler) および第1のリンク情報付き役割識別子により新たに発信者リンク情報付き役割識別子を変更し、第3のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0124】

請求項53記載の本発明にあっては、第1のリンク指定型個別化アクセスチケットの所有者リンク情報付き役割識別子を第1の個別化アクセスチケット変更権(Enabler) で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler) および第1のリンク情報付き役割識別子により新たな発信者リンク情報付き役割識別子を変更し、第3のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0125】

更に、請求項54記載の本発明は、個別化アクセスチケット変更権(Enabler) により第3の機関において会員を追加する方法を実施するプログラムを記録した記録媒体であって、第4のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第3の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler) 、1個以上の第2のリンク情報付き役割識別子により1個以上の新たな着信者リンク情報付き役割識別子に追加し、第5のリンク情報付き個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0126】

請求項54記載の本発明にあっては、第4のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第3の個別化アクセスチケット変更権(Enabler) と照合し、正しい場合に、1個以上の第4の個別化アクセスチケット変更権(Enabler) 、1個以上の第2のリンク情報付き役割識別子により1個以上の新たな着信者リンク情報付き役割識別子に追加し、第5のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0127】

請求項55記載の本発明は、個別化アクセスチケット変更権(Enabler)により第3の機関において会員を削除する方法を実施するプログラムを記録した記録媒体であって、第6のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3のリンク情報付き役割識別子により1個以上の着信者リンク情報付き役割識別子を削除し、第7のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録することを要旨とする。

【0128】

請求項55記載の本発明にあつては、第6のリンク指定型個別化アクセスチケットの発信者リンク情報付き役割識別子を第4の個別化アクセスチケット変更権(Enabler)と照合し、正しい場合に、1個以上の第5の個別化アクセスチケット変更権(Enabler)、1個以上の第3のリンク情報付き役割識別子により1個以上の着信者リンク情報付き役割識別子を削除し、第7のリンク指定型個別化アクセスチケットを作成する接続制御プログラムを記録媒体に記録するため、該記録媒体を用いて、その流通性を高めることができる。

【0129】

また、請求項56記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、リンク指定型個別化アクセスチケットが、発信者フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第3の機関の秘密鍵による署名から構成されるリンク指定型1対1個別化アクセスチケットであり、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報および第1の機関の秘密鍵による署名から構成され、個人識別子が、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0130】

請求項56記載の本発明にあつては、発信フラグ、移転制御フラグ、発信者リンク情報付き役割識別子のリンク情報、着信者リンク情報付き役割識別子のリンク情報、有効期限、および第3の機関の秘密鍵による署名から構成されるリンク指定型1対1個別化アクセスチケットを発信者と着信者の1対1対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0131】

更に、請求項57記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であつて、リンク指定型個別化アクセスチケットが、発信者Index、所有者Index、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク指定型1対N個別化アクセスチケットであり、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報、および第1の機関の秘密鍵による署名から構成され、個人識別子が、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0132】

請求項57記載の本発明にあつては、発信者Index、所有者Index、移転制御情報、発信者リンク情報付き役割識別子のリンク情報、1個以上の着信者リンク情報付き役割識別子のリンク情報、および有効期限情報から構成されるリンク情報付き1対N個別化アクセスチケットを発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0133】

請求項58記載の本発明は、個別化アクセスチケット変更権(Enabler)を記録したコンピュータで読み取り可能な記録媒体であつて、個別化アクセスチケット

変更権(Enabler)が、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第1の機関の秘密鍵による署名から構成され、リンク情報付き役割識別子が、個人識別子、暗号化された位置情報、第4の機関のホスト個人情報、リンク情報、および第1の機関の秘密鍵による署名から構成され、個人識別子が、第1の機関が一意に付与した文字列、および第1の機関の秘密鍵による署名から構成され、発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報を特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0134】

請求項58記載の本発明にあつては、個別化アクセスチケット変更権(Enabler)であることを一意に表す文字列、役割識別子、および第1の機関の秘密鍵による署名から構成される個別化アクセスチケット変更権(Enabler)を発信者と着信者の1対N対応に指定しているユーザ間の接続制御情報としてコンピュータで読み取り可能に記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0135】

また、請求項59記載の本発明は、リンク指定型個別化アクセスチケット(PAT)の新規生成および既存のリンク指定型個別化アクセスチケット(PAT)の内容変更を行うため、Null-AID(AID_{Null})および該Null-AIDのEnabler(Enabler of Null-AIDまたはEnabler of AID_{Null})を使用し、該Null-AIDを含む演算は、

(a) リンク指定型個別化アクセスチケット(PAT)に対する新規生成(Make PAT)、マージ(Merge PAT)、分割(Split PAT)、変更(Trans PAT)からなる演算規則に従い、

(b) Null-AIDにのみ適用可能な規則として、

i. Null-AIDは、すべてのユーザに既知であり、

ii. Enabler of Null-AIDは、すべてのユーザに既知である

ことを要旨とする。

【0136】

請求項59記載の本発明にあっては、リンク指定型個別化アクセスチケット（PAT）の新規生成および既存のリンク指定型個別化アクセスチケット（PAT）の内容変更を行うために、Null-AID（AID_{Null}）および該Null-AIDのEnabler（Enabler of Null-AIDまたはEnabler of AID_{Null}）を使用するため、会員AIDおよびEnablerr of 会員AIDを所有者AIDに渡さなくても新規生成（MakePAT）およびマージ（MergePAT）を行うことができる。

【0137】

更に、請求項60記載の本発明は、請求項59記載の発明において、前記Null-AIDは、リンク指定型個別化アクセスチケット（PAT）の所有者AIDとしてのみ使用可能であり、

【数12】

$PAT < AID_{Null} | AID_{\text{会員1}}, AID_{\text{会員2}}, \dots, AID_{\text{会員N}} >$
は許可することを要旨とする。

【0138】

請求項60記載の本発明にあっては、Null-AIDはリンク指定型個別化アクセスチケット（PAT）の所有者AIDとしてのみ使用可能であり、

【数13】

$PAT < AID_{Null} | AID_{\text{会員1}}, AID_{\text{会員2}}, \dots, AID_{\text{会員N}} >$
は許可するため、 $PAT < AID_{\text{所有者}} | AID_{\text{会員}} >$ の所有者がAID_{会員の}Enablerを知らない場合には、このPATから $PAT < AID_{Null} | AID_{\text{会員}} >$ を作成することはできない。

【0139】

請求項61記載の本発明は、God-AID（AID_{God}）を用いて、リンク指定型個別化アクセスチケット（PAT）に読取専用属性を設定し、該God-AIDに関する演算は、

- (a) God-AIDは、すべてのユーザに既知であり、
- (b) God-AIDに関する演算が、

【数14】

i. AID所有者がAID_{Null}でもAID_{God}でもない場合:

PAT < AID所有者 | AID_{会員1}, AID_{会員2},
..., AID_{会員N} >

+ Enabler of AID所有者

→ PAT < AID_{God} | AID所有者, AID_{会員1}, AID_{会員2},
..., AID_{会員N} >

ii. AID所有者がAID_{Null}の場合:

PAT < AID_{Null} | AID_{会員1}, AID_{会員2},
..., AID_{会員N} >

+ Enabler of AID_{Null}

→ PAT < AID_{God} | AID_{会員1}, AID_{会員2},
..., AID_{会員N} >

である場合のいずれかのみ許可されることを要旨とする。

【0140】

請求項61記載の本発明にあっては、God-AID (AID_{God}) を用いて、リンク指定型個別化アクセスチケット (PAT) に読取専用属性を設定するため、グループ通信において参加者を固定することができる。

【0141】

また、請求項62記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Null-AIDが、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0142】

請求項62記載の本発明にあっては、Null-AIDであることを表す文字列および該文字列に対して認証局の署名を施したのからなるデータ構造のNull-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0143】

更に、請求項63記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であって、Enabler of Null-AIDが、Enablerであることを表す文字列、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0144】

請求項63記載の本発明にあつては、Enablerであることを表す文字列、Null-AIDの実体、およびEnablerであることを表す文字列とNull-AIDの実体を連結した文字列に対して認証局の署名を施したものであるデータ構造のEnabler of Null-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0145】

請求項64記載の本発明は、リンク指定型個別化アクセスチケットを記録したコンピュータで読み取り可能な記録媒体であつて、God-AIDが、God-AIDであることを表す文字列および前記God-AIDであることを表す文字列に対して認証局の署名を施したものであることを特徴とするデータ構造を記録媒体に記録することを要旨とする。

【0146】

請求項64記載の本発明にあつては、God-AIDであることを表す文字列およびGod-AIDであることを表す文字列に対して認証局の署名を施したものであるデータ構造のGod-AIDを記録媒体に記録しているため、該記録媒体を用いて、その流通性を高めることができる。

【0147】

【発明の実施の形態】

以下、図面を用いて本発明の第1の実施の形態について説明する。本発明の接続制御方法は、通信網における発信者および着信者の匿名性を保持しつつ、発信者からの通信をも適宜可能とするものであり、基本的には着信者の本当の識別子

を隠蔽した状態で、着信者の特性を表す情報のみを公開し、この公開された情報に基づいて、匿名性を保持したまま通信を希望する者に対して限定的なアクセス権を付与することにある。

【0148】

具体的には、図1(a)に示すように、ユーザに対して個人情報を隠蔽した役割識別子(Anonymous Identification: AIDと略称する)を付与し、この役割識別子AIDをユーザの特性を表す情報である趣味、年齢、職業等のようなユーザをネットワーク上で特定はできないが、発信者にとって当該ユーザと通信する価値があるかどうかを判断するための有用な情報と組にしてネットワークに公開する。

【0149】

また、発信者は、前記公開された情報を閲覧または検索することにより自分が通信したい相手を捜すことができる。すなわち、発信者が発信者自身の匿名性を保持したままある相手と通信したい場合には、その相手の役割識別子を指定し、個別化アクセスチケットPAT(Personalized Access Ticket)を取得する。

【0150】

個別化アクセスチケットPATには、後述する図3(c)に示すように、発信者、着信者それぞれの役割識別子AIDの他に、発信者フラグ、移転制御フラグ、および、有効期限の各情報が記載されている。移転制御フラグは、図1(b)、(c)に示すように着信拒否等の接続制御を行うために使用される。すなわち、移転制御フラグを立てると、後述するセキュア・コミュニケーション・サービスSCS(Secure Communication Service)は、接続要求の際に、発信者に対し、例えば署名の検証、パスワード要求等の認証を行う。また、移転制御フラグを立てない場合には、セキュア・コミュニケーション・サービスSCSは認証無しで接続要求をセキュア・コミュニケーション・サービスSCSが接続している物理的通信網に渡す。すなわち、移転制御は役割識別子AIDがこれを認証局CA(Certification Authority)から割り当てられたユーザによって正当に利用されているかを認証するために用いられる。

【0151】

本発明の接続制御方法を実施する通信網においては、ユーザに対する役割識別子AIDの付与、役割識別子AIDと組み合わされた情報の保持、個別化アクセスチケットPATの発行、および個別化アクセスチケットPATに基づく接続制御はそれぞれ別の機関で行われている。これは、それぞれの行為に関して保持すべきセキュリティレベルに差があるので、別々の機関で実行した方がネットワーク全体のセキュリティの保持には好都合だからである。

【0152】

図2は、本発明の一実施形態の全体構成図である。本実施形態はインターネット電子メールシステムを対象としたものである。図2において、1は認証局CAであり、認証権限と役割識別子AIDの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。3はユーザであり、5はセキュア・コミュニケーション・サービスSCSであり、ユーザ3間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。7はアノニマス・ディレクトリ・サービスADSであり、役割識別子AID、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスADS7は、検索者の役割識別子AIDと検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子AIDから個別化アクセスチケットPATを発行し、検索者に交付する機能を有する。

【0153】

まず、ユーザの要求に基づいて個人識別子から役割識別子AIDを生成し、そのユーザに割り当てるまでの一連の処理について説明する。

【0154】

図3は、個人識別子OID(Official Identification)、役割識別子AIDおよび個別化アクセスチケットPATの例を示している。同図に示すように、個人識別子OIDは、図3(a)に示すように認証局CA1がユーザに一意に生成した任意の文字列に対して認証局CA1が秘密鍵で電子署名したものである。また、役割識別子AIDは、図3(b)に示すように個人識別子OIDの一部とその位置情報、冗長な文字列、SCSのホストOIDからなる文字列に対し、認証局

CA1の秘密鍵で電子署名を施したものである。

【0155】

また、個別化アクセスチケットPATは、図3(c)に示すように、発信者フラグ、移転制御フラグ、役割識別子AID₀、役割識別子AID₁、有効期限からなる文字列に対してアノニマス・ディレクトリ・サービスADSのOID秘密鍵による電子署名を施したものである。なお、この個別化アクセスチケットを以下1対1個別化アクセスチケットと称することにする。

【0156】

更に、後述する各実施形態で説明するように、本発明は、個別化アクセスチケットPATとして、上述した1対1個別化アクセスチケットに加えて、発信者と着信者を1対Nに対応させている1対N個別化アクセスチケット、および役割識別子の実体を個別化アクセスチケットで指定する代わりに役割識別子を指定するリンク情報を持ち、このリンク情報で役割識別子を指定するリンク指定型個別化アクセスチケットを有し、このリンク指定型個別化アクセスチケットには上述した発信者と着信者の対応関係に基づきリンク指定型1対1個別化アクセスチケットとリンク指定型1対N個別化アクセスチケットがある。すなわち、本発明の個別化アクセスチケットには、1対1個別化アクセスチケット、1対N個別化アクセスチケット、リンク指定型1対1個別化アクセスチケット、およびリンク指定型1対N個別化アクセスチケットの4種類がある。

【0157】

次に、ユーザ3が役割識別子AIDを認証局CA1に対して請求する処理について図4に示すフローチャートを参照して説明する。ユーザは個人識別子OIDと請求項目を入力して(ステップS411)、図7に示すようにAID請求メッセージを作成し(ステップS413)、ユーザOIDの秘密鍵で署名、暗号化し(ステップS415)、それから該AID請求メッセージを認証局CA1に電子メールで送信する(ステップS147)。

【0158】

AID請求メッセージは、発信者の個人識別子OIDと請求項目から構成され、請求項目は次に示す2種類のうちのいずれかである。

【0159】

(1) 新規な役割識別子AIDの割り当てを要求する場合：

REQUEST AID <要求するAIDの数>

(2) 既存の役割識別子AIDの廃止を要求する場合：

DISCARD AID <廃止したいAIDの実体>

次に、上述した役割識別子AIDの請求に対する認証局CA1が役割識別子AIDをユーザ3に対して交付する処理について図5に示すフローチャートを参照して説明する。図5において、認証局CA1は、ユーザ3からの上述したAID請求メッセージを受信すると（ステップS511）、認証局CA1はユーザ3のOID公開鍵を用いてAID請求メッセージ（図7）を復号化、認証する（ステップS513）。認証局CA1は該メッセージが改竄されているか否かをチェックする（ステップS515）。改竄を検出した場合には、該メッセージを破棄するが、改竄が認められなかった場合には、認証局CA1は役割識別子AIDを生成し（ステップS517）、AID秘密鍵およびAID公開鍵を生成し（ステップS519）、図8に示すAID交付メッセージを生成する（ステップS521）。それから、認証局CA1は該メッセージをユーザOIDの公開鍵で署名、暗号化し（ステップS523）、この署名したメッセージをユーザ3のOIDに送信する（ステップS525）。

【0160】

次に、図6に示すフローチャートを参照して、ユーザにおけるAID交付処理について説明する。図6において、ユーザ3が認証局CA1からの暗号化されたAID交付メッセージを受信すると（ステップS611）、ユーザ3はユーザ秘密鍵を用いてAID交付メッセージを復号化、認証し（ステップS613）、該メッセージが改竄されているか否かをチェックする（ステップS615）。改竄を検出した場合には、エラーメッセージを出力し、該AID交付メッセージを破棄する（ステップS617）。また、改竄が認められない場合には、AID交付メッセージから役割識別子AIDとAID秘密鍵を抽出し、ユーザ3に通知する（ステップS619）。

【0161】

AID交付メッセージは、図8に示すように発信者OIDと処理結果から構成されている。処理結果は次に示す2種類のうちのいずれかである。

【0162】

(1) 新規な役割識別子AIDの交付の場合：

NEW AID <新規AIDの実体とAIDの秘密鍵 | AID取得失敗>

(2) 既存の役割識別子AIDの廃止

DISCARD AID <既存AIDの実体><廃止完了 | 廃止失敗>

次に、認証局CAにおける役割識別子AIDの生成処理について図9、図10を参照して説明する。図9において、認証局CA1は乱数発生等の任意の手段を用いて、個人識別子OIDの全長Lと等しい長さの文字列を生成し、この文字列を仮の役割識別子AIDとして生成する（ステップS911）。

【0163】

次に、個人識別子OIDの複写を行うために、個人識別子OIDのコピー範囲を指定するpとlの値を決定する（ステップS913）。これは、乱数発生等の任意の手段を用いて、パラメータ p_i と l_i の値をそれぞれ $0 \leq p_i \leq L$ および $l_{\min} \leq l_i \leq l_{\max}$ のようにコピー範囲を決定する。ここで、Lは個人識別子OIDの全長であり、 l_{\min} および l_{\max} は $0 < l_{\min} < l_{\max} < L$ が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子OIDの先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにコピー範囲を設定する。次に、図10（a）、（b）に示すように、ペースト先頭位置を仮の役割識別子AIDの先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにペースト位置を設定する。

【0164】

それから、図10（a）、（b）に示すように、上述したコピー範囲の文字列を仮の役割識別子AIDの上述したペースト位置に上書きして複写する（ステップS915）。このように上書きした文字列の特定の位置に位置情報 p_i および l_i の値を、CAが定めた方法で暗号化して、図10（c）で指定した位置に付加し（ステップS917）、更にこの位置情報を付加した文字列にセキュア・コ

コミュニケーション・サービスSCSのホストOID（ホスト名、ドメイン名、またはIPアドレス）を図10（c）に示すように付加する（ステップS919）。そして、このようにセキュア・コミュニケーション・サービスSCSのホストOIDを付加した文字列に認証局CAのOID秘密鍵で電子署名を施す（ステップS921）。

【0165】

次に、役割識別子AIDによる個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービスADS7において、個人情報を登録するまでの流れを図11（a）に示す。同図に示すように、登録者であるユーザB3は自らの役割識別子AID、移転制御情報、有効期限、および、性別、年齢、趣味等のプライバシー情報をアノニマス・ディレクトリ・サービスADS7に送付する。

【0166】

また、アノニマス・ディレクトリ・サービスADS7における検索処理を図11（b）に示す。検索者であるユーザA3は、自らの役割識別子AIDと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスADS7に送信する。アノニマス・ディレクトリ・サービスADS7は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子AIDを抽出する。アノニマス・ディレクトリ・サービスADS7は最後に検索者の役割識別子AIDと検索条件にマッチした登録者の役割識別子AIDから個別化アクセスチケットPATを生成し、検索者であるユーザA3に交付する。

【0167】

1対1個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスADS7の検索結果として生成する。

【0168】

次に、図12のフローチャートを参照して、ADSにおけるPAT生成処理について説明する。

【0169】

1. 検索者AID秘密鍵で署名された検索者AIDを入力する（ステップS1210）。
2. ステップS1210における検索者AIDをその検索者AIDの公開鍵で認証する（ステップS1211）。

【0170】

3. ステップS1211における認証の結果
 - ・ 検索者AIDが改竄されている場合処理を中止する。
 - ・ 検索者AIDが改竄されていない場合、ステップS1215に進む。
4. ステップS1211で認証済みの検索者AIDを、登録者AID（ADS登録時に登録者AIDの秘密鍵で認証済み）と連結する（ステップS1215）。
5. ステップS1215で連結した、検索者AIDと登録者AIDからなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定する。また、発信者フラグを「0」と設定する（ステップS1217）。
6. ステップS1217の結果に、ADSのOID秘密鍵で署名する（ステップS1219）。
7. ステップS1219の結果（つまり、PAT）を、検索者AIDに送信する（ステップS1221）。

なお、PATを受信した検索者は、ADSのOID公開鍵を用いて受信したPATを認証し、改竄されていないければ、これを検索者端末の記憶装置に記憶し、改竄されていれば、破棄します。この手順は、図6と同様である。

【0171】

次に、1対1個別化アクセスチケットPATによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子AIDと実際の発信者を対応付けられるようにすることである。

【0172】

アノニマス・ディレクトリ・サービスADS7および着信者は、個別化アクセスチケットPATの移転制御フラグを設定することにより、発信者に番号通知さ

せるか否かを選択させることができる。

【0173】

移転制御フラグを「1」に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われるため、着信者は発信者の役割識別子AIDと実際の発信者を対応付けることができる（発信者番号通知）。また、移転制御フラグを「0」に設定した場合には、着信者は発信者の役割識別子AIDと実際の発信者を対応付けることができない（発信者番号非通知）。

【0174】

図14のフローチャートを参照して、SCSにおけるメール接続制御の処理手順について説明する。

【0175】

1. メールを入力する（ステップS1411）。
2. ステップS1411のメールのTo:フィールドからPATを抽出する。次に、このPATに対するADS公開鍵をADSに何らかの手段で問い合わせ、そのADS公開鍵を取得する。そして、PATをADS公開鍵で認証する（ステップS1413）。

【0176】

3. ステップS1413における認証の結果
 - ・PATが改竄されている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する（ステップS1429）。
 - ・PATが改竄されていない場合、ステップS1417に進む。
4. ステップS1411のメールのFrom:フィールドから発信者AIDを抽出する。また、メールのTo:フィールドのPATの移転制御フラグを解析し、PATから発信者AIDを抽出する（ステップS1417, S1419）。
5. ステップS1417, S1419で抽出した発信者AID同士を比較する（ステップS1421）。

【0177】

6. ステップS1421における比較の結果

- ・両者が一致しない場合ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する(ステップS1429)。

- ・両者が一致する場合、ステップS1425に進む。

7. ステップS1411のメールのTo:フィールドのPATから有効期限を抽出する(ステップS1425)。

8. ステップS1411のメールのTo:フィールドのPATが有効期限内かどうかを検証する(ステップS1427)。

9. ステップS1427における検証の結果

- ・有効期限を過ぎている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する(ステップS1429)。

- ・有効期限内の場合、ステップS1431に進む。

10. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を調べる。

11. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を抽出する(ステップS1431)。

【0178】

12. ステップS1431における抽出の結果

- ・移転制御フラグ値が「1」の場合、図15～図17の手順に従い、移転制御を行ってから(ステップS1435)、図18の手順に従い、メールを着信者AID宛に転送する(ステップS1437)。

- ・移転制御フラグ値が「0」の場合、図18の手順に従い、メールを着信者AID宛に転送する(ステップS1437)。

この移転制御について図15～図17を参照して説明する。まず、図15において、セキュア・コミュニケーション・サービスSCS5は、個別化アクセスチケットPATを入力すると(ステップS1511)、それから、セキュア・コミュニケーション・サービスSCS5は、任意の文字列、例えばタイムスタンプを生成し(ステップS1517)、この生成した文字列を発信者の役割識別子AI

Dに送信する（ステップS1519）。

【0179】

ユーザにおいては、図16に示すように、前記文字列を受信すると（ステップS1611）、この文字列に発信者役割識別子AIDの秘密鍵で署名し（ステップS1613）、署名つき該文字列をセキュア・コミュニケーション・サービスSCS5に送信する（ステップS1615）。

【0180】

セキュア・コミュニケーション・サービスSCS5においては、図17に示すように、署名つき前記文字列を受信すると（ステップS1711）、発信者の役割識別子AIDの公開鍵で認証し（ステップS1713）、改竄されているか否かをチェックする（ステップS1715）。改竄されている場合には、改竄されている旨を何らかの手段で発信者AIDに通知してからアボート（異常終了）するが（ステップS1717）、改竄されていない場合には、セキュア・コミュニケーション・サービスSCS5は、図18に示す接続制御を行う。

【0181】

以下、図18のフローチャートを参照して接続制御について説明する。

【0182】

1. メールのTo:フィールドのPATから、発信者のSCSホストOIDと着信者のSCSホストOIDを抽出する（ステップS1811）。
2. ステップS1811で抽出した発信者、着信者それぞれのSCSホストOIDのデータ形式を調べる（ステップS1813）。

【0183】

3. ステップS1813における調査の結果

・発信者SCSホストOIDと着信者SCSホストOIDのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップS1815に進み、ホスト名またはドメイン名で与えられているSCSホストOIDをDNS(Domain Name Service)に問い合わせ、そのホスト名またはドメイン名に対するIPアドレスを取得してから、ステップS1817に進む。

【0184】

・発信者SCSホストOIDと着信者SCSホストOIDがともにIPアドレスで与えられている場合には、そのままステップS1817に進む。

4. ステップS1815, S1817で抽出あるいは変換したIPアドレスを比較する(ステップS1817)。

【0185】

5. ステップS1817における比較の結果

・発信者SCSホストOID(IPアドレス)と着信者SCSホストOID(IPアドレス)が一致する場合、ステップS1819からステップS1823に進み、発信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する(ステップS1823)。この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1825からステップS1827に進み、ステップS1811のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0186】

また、ステップS1825において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、着信者AIDを検索条件として、着信拒否データベースに問い合わせる(ステップS1829)。

【0187】

この問い合わせの結果、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1831からステップS1827に進み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0188】

また、ステップS1831において、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納

して正常終了する(ステップS1833)。

【0189】

一方、ステップS1819において、発信者SCSホストOID(IPアドレス)と着信者SCSホストOID(IPアドレス)が一致しない場合、について説明する。

【0190】

まず、SMTPに従い、メールを着信者AIDをアカウントに持つSCSホストに転送する(ステップS1835)。

【0191】

次に、着信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する(ステップS1837)。

【0192】

この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1839からステップS1841に進み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0193】

また、ステップS1839において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、ステップS1843に進む。ステップS1843では着信者AIDを検索条件として、着信拒否データベースに問い合わせる。

【0194】

ステップS1843における問い合わせの結果、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1845からステップS1841に進み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0195】

また、ステップS1845において、メールのTo:フィールドのPAT、ま

たは、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されていない場合、ステップS1847に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【0196】

図19のフローチャートを参照して、SCSにおけるメール返信処理について説明する。

【0197】

1. エラーを検出したSCSホストは、PAT<エラーを検出したSCSホストOID | From: フィールドの発信者AID>を生成する(ステップS1911)。
2. ステップS1911のSCSホストは、ステップS1911で生成したPATを、エラーが発生したメールのTo: フィールドにセットする(ステップS1913)。
3. ステップS1911のSCSホストは、ステップS1913でセットしたメールを(発信者AID宛に)送信する(ステップS1915)。

【0198】

次に、個別化アクセスチケットPATに対する着信拒否について説明する。

【0199】

着信者AID側で指定した個別化アクセスチケットPATがTo: フィールドに記述されたメールが、着信者AIDに含まれるホストOIDのセキュア・コミュニケーション・サービスSCS5に到着した場合には、そのセキュア・コミュニケーション・サービスSCS5はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者AID宛に返信する。この一連の処理を着信拒否と呼ぶ。

【0200】

ユーザにおける着信拒否申請処理について図22に示すフローチャートを参照して説明する。ユーザは役割識別子AIDと個別化アクセスチケットPATを入力し(ステップS2211)、図24の上側に示す着信拒否申請メッセージを作成し(ステップS2213)、着信者AIDの秘密鍵で署名、暗号化する(ステ

ップS2215)。それから、着信者はこの暗号化した申請メッセージをセキュア・コミュニケーション・サービスSCS5に送信する(ステップS2217)。

【0201】

着信拒否申請メッセージは、図24の上側に示すように、着信者の役割識別子AIDと申請項目から構成される。申請項目は次の2種類のうちのいずれかである。

【0202】

(1) 着信拒否の設定

<着信者AIDの実体>REFUSE<PATの実体、IPアドレス、ドメイン名、ホスト名>

(2) 着信拒否の解除

<着信者AIDの実体>RECONNECT <PATの実体、IPアドレス、ドメイン名、ホスト名>

【0203】

次に、図23に示すフローチャートを参照して、セキュア・コミュニケーション・サービスSCS5における着信拒否設定処理について説明する。セキュア・コミュニケーション・サービスSCS5は、着信拒否申請メッセージを受け取ると(ステップS2311)、着信者のAID公開鍵で認証し(ステップS2313)、改竄されているか否かをチェックする(ステップS2315)。改竄されていない場合には、着信拒否メッセージから個別化アクセスチケットPAT、IPアドレス、ドメイン名、またはホスト名を抽出し(ステップS2317)、該個別化アクセスチケットPAT、該IPアドレス、該ドメイン名、該ホスト名を着信拒否データベース(DB)に登録(または削除)する(ステップS2319)。それから、図24の下側に示すような着信拒否通知メッセージを生成し(ステップS2321)、着信者AID公開鍵で署名、暗号化し(ステップS2323)、この暗号化されたメッセージを着信者AIDに返信する(ステップS2325)。

【0204】

着信拒否通知メッセージは、図24の下側に示すように、着信者の役割識別子AIDと処理結果から構成されている。処理結果は次に示す2種類のうちのいずれかである。

【0205】

(1) 着信拒否の設定結果

<着信者AIDの実体>REFUSE<成功 | 失敗><PATの実体、IPアドレス、ドメイン名、ホスト名>

(2) 着信拒否の解除結果

<着信者AIDの実体>RECONNECT <成功 | 失敗><PATの実体、IPアドレス、ドメイン名、ホスト名>

着信拒否の実行に当たっては、セキュア・コミュニケーション・サービスSCSSは、個別化アクセスチケットPATを着信拒否データベースに問い合わせる。該当個別化アクセスチケットが存在する場合、または、発信者AIDに、該当するIPアドレス、ホスト名、ドメイン名が含まれる場合には、メールを発信者AIDに返信する。存在しない場合には、メッセージを着信者アカウントのメールボックスまたはスプールに格納する。

【0206】

図25のフローチャートを参照して、同一性の判定について説明する。

【0207】

1. 変数OID_Mの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する。また、変数OID_Vの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する（ステップS2511）。

【0208】

2. 処理対象のAIDの集合から1個のAIDを選択し、以下のビット演算を実行する（ステップS2513）。

【0209】

(a) AIDに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの

値を決定する（ステップS2515）。ここで、

- ・ AID_M はOIDの全長Lと等しい長さで、かつ、
 - －OID情報が定義されている位置の値は1である。
 - －OID情報が定義されていない位置の値は0である。
- ビット列と定義する（図26）。

【0210】

- ・ AID_V はOIDの全長Lと等しい長さで、かつ、
 - －OID情報が定義されている位置の値はOID情報の実際の値である
 - －OID情報が定義されていない位置の値は0である。
- ビット列と定義する（図26）。

【0211】

(b) OID_M と AID_M のAND演算を実行し、その結果を変数 OVR_M に代入する（ステップS2517）。

【0212】

(c) OVR_M と AID_M のAND演算と、 OVR_M と OID_M のAND演算を実行し、その演算結果を比較する（ステップS2519）。

- ・一致する場合 OID_M と AID_M のOR演算を実行し、実行結果を OID_M に代入する（ステップS2521）。また、 OID_V と AID_V のOR演算を実行し、実行結果を OID_M に代入する（ステップS2523）。

- ・一致しない場合、ステップS2525に進み、実行する。

【0213】

(d) 処理対象のAIDの集合から、次に処理するAIDを抽出する。

- ・集合に少なくとも1個のAIDが含まれている場合、ステップS2519を実行する。

- ・集合にAIDが1個も含まれていない場合、ステップS2527に進む。

【0214】

(e) OID_M および OID_V の値を出力する（ステップS2527）。

最終的に得られた OID_M の値は、処理対象のAIDの集合から復元できたOID情報のすべての位置を表している。また、最終的に得られた OID_V の値は

、処理対象のAIDの集合から復元できたOID情報のすべてを表している。つまり、 OID_M と OID_V の値を用いると、

(a) OID_V の値を検索条件とすると、確率的にはあるがOIDを求めることができる。

【0215】

(b) 上記検索の精度を、OID全長Lとの比 $OID_M L$ で定量的に評価することができる。

【0216】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子OIDからこれらの情報を隠蔽した役割識別子AIDを作成すべく図7に示すような役割識別子AID請求メッセージを作成し、認証局CA1に送信すると、認証局CA1は、該メッセージを受け取って、役割識別子AIDを生成し、ユーザに交付する。

【0217】

ユーザは、この交付された役割識別子AIDおよび性別、年齢、趣味等の個人情報情報をアノニマス・ディレクトリ・サービスADS7に送信し、アノニマス・ディレクトリ・サービスADS7に役割識別子AIDと個人情報を登録する。このように登録された情報を検索する場合は、検索者は自己の役割識別子AIDと検索条件（性別、年齢、趣味等のプライバシー情報）をアノニマス・ディレクトリ・サービスADS7に送信する。アノニマス・ディレクトリ・サービスADS7は、これらの情報を受信すると、該検索条件にマッチした登録者の役割識別子AIDを抽出する。そして、アノニマス・ディレクトリ・サービスADS7は、検索者の役割識別子AIDと検索条件にマッチした登録者の役割識別子AIDから1対1個別化アクセスチケットPATを生成し、検索者に交付する。

【0218】

この1対1個別化アクセスチケットPATには、図3(c)に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【0219】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者A I Dと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを1に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われ、着信者は発信者A I Dと実際の発信者を対応付けることができる（発信者番号通知）。また、該フラグを0に設定した場合は、移転制御は行われず、着信者は発信者A I Dと実際の発信者を対応付けることはできない（発信者番号非通知）。

【0220】

また、1対1個別化アクセスチケットP A Tで着信者を指定した呼を個別化アクセスチケットP A T内で定義した着信者役割識別子A I Dまたは発信者役割識別子A I Dに着信するように、通信網に対して接続要求をすることができる。更に、1対1個別化アクセスチケットP A Tで指定した呼のうち、着信者が選択した1対1個別化アクセスチケットP A Tの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子A I Dで個人攻撃を繰り返す発信者への対処として、それら複数の発信者役割識別子A I Dから個人識別子O I Dの同一性を判定することができ、かつ、その個人識別子のある確率で取り出すことができる。

【0221】

次に、本発明の第2の実施形態に係る接続制御方法について図31乃至図60を参照して説明する。上述した第1の実施形態では発信者と着信者を1対1に対応させるとともに、偽装防止のためにユーザ要求に基づいた個別化アクセスチケットの新規生成、内容変更を許可していない場合について説明したのに対して、第2の実施形態では、発信者と着信者を1対Nに対応させるとともに、この1対N個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者および着信者は所有者または会員である。

【0222】

一般に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス、インターネットメールアドレス等の連絡先情報を管理する必要がある。これに対して、第1の実施形態のように、個別化アクセスチケットの新規生成、内容変更ができない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【0223】

本第2の実施形態では、このような不具合を解消するために1対N個別化アクセスチケットPATの新規生成および既存の1対N個別化アクセスチケットPATの内容変更をユーザ主導でできるようにしている。

【0224】

まず、本第2の実施形態で使用される各識別子の定義について図31、図32を参照して説明する。

【0225】

個人識別子（Official Identification：OID）は、図31（a）に示すように、認証局（Certificate Authority：CA）が任意に生成した文字列（電話番号、電子メールアドレス等）、または前記文字列に対しCA秘密鍵で電子署名を施したものである。

【0226】

役割識別子（Anonymous Identification：AID）は、図31（b）に示すように、OIDの一部とその位置情報、任意に生成した冗長な文字列、SCSのホストOIDからなる文字列に対し、CA秘密鍵で電子署名を施したものである。また、AIDはSCSやCAで暗号化する場合もある。

【0227】

個別化アクセスチケット（Personalized Access Ticket：PAT）は、図31（c）に示すように、1個の所有者AID（Holder AID）、1個以上の会員AID（Member AID）、発信者インデックス、所有者インデックス、有効期限情

報、移転制御情報、PAT演算装置識別子から構成されるリストに対し、PAT演算装置識別子の秘密鍵で署名したものである。ここで、発信者インデックスは、AIDリスト中の発信者AIDの位置を表す数値データで、先頭AIDが発信者AIDであれば1、2番目ならば2、…、n番目ならばnである。所有者インデックスは、AIDリスト中の所有者AIDの位置を表す数値データで、先頭AIDが所有者AIDであれば1、2番目ならば2、…、n番目ならばnであると定義する。移転制御情報は、移転可の場合は「0」という数値、また移転不可の場合は「1」という数値のいずれかで表す。

【0228】

所有者AIDは、AIDリスト中の所有者インデックスで指定した位置に書き込まれているAIDである。会員AIDは、所有者AID以外のすべてのAIDである。有効期限情報は、数値データであって、使用可能回数、PATが利用不可能になる絶対時刻(UTC)、PATが利用可能になる絶対時刻(UTC)、PATが利用可能になってから利用不可能になるまでの相対時間(寿命)のいずれか、または複数を組み合わせて記述する。PAT演算装置識別子は、PAT演算装置のシリアルナンバーである。PAT演算装置の秘密鍵は、上記シリアルナンバーに対する秘密鍵である。これらの中で、所有者AIDと会員AIDからなる部分を以後、AIDリストと呼ぶことにする。

【0229】

また、本第2の実施形態では、所有者役割識別子AIDに対応した識別子として、Enablerを導入している。Enablerは、図32に示すように、Enablerであることを通信網上で一意に表す文字列とAIDからなる文字列に対して、CA秘密鍵で電子署名したものである。

【0230】

次にPATの新規生成および内容変更における操作について説明する。通信端末上のセキュアなPAT演算装置、CA上もしくはCAから正当に依頼されたネットワーク上のPAT演算オブジェクト(以後、これもPAT演算装置と呼ぶことにする)において、次の操作が定義される。

【0231】

(1) AIDリストの演算：

所有者AIDおよび所有者AIDに対応するEnabler を用いて、AIDリストを新規生成あるいは変更する。

(2) 有効期限情報および移転制御情報の設定：

所有者AIDおよび所有者AIDに対応するEnabler を用いて、有効期限情報および移転制御情報を設定もしくは変更する。

【0232】

所有者AIDに対してのみAIDリストの演算を許可するために、以下の演算規則を定義する。

【0233】

(1) 新規生成 (MakePAT) (図33参照)：

AIDリスト (ALIST<所有者AID | 会員AID₁, 会員AID₂, ..., 会員AID_n>) を新規生成し、生成後のALISTに対し、有効期限情報および移転制御情報を設定する。

【0234】

【数15】

$$\begin{aligned} & AID_A + AID_B + \text{Enabler of } AID_B + \text{Enabler of } AID_A \\ \rightarrow & ALIST<AID_A | AID_B> ALIST<AID_A | AID_B> \\ & + \text{Enabler of } AID_A + \text{有効期限情報} + \text{移転制御情報} \\ \rightarrow & PAT<AID_A | AID_B> \end{aligned}$$

(2) マージ (MergePAT) (図34参照)：

同一所有者AIDの複数ALISTをマージし、マージ後のALISTに対し、有効期限情報および移転制御情報を設定する。

【0235】

【数16】

$$\begin{aligned} & ALIST<AID_A | AID_{B1}, AID_{B2}, \dots> \\ & + ALIST<AID_A | AID_{C1}, AID_{C2}, \dots> \\ & + \text{Enabler of } AID_A \end{aligned}$$

$$\begin{aligned} &\rightarrow \text{ALIST} \langle \text{AID}_A \mid \text{AID}_{B1}, \text{AID}_{B2}, \dots, \\ &\quad \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\text{ALIST} \langle \text{AID}_A \mid \text{AID}_{B1}, \text{AID}_{B2}, \dots, \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\quad + \text{Enabler of AID}_A + \text{有効期限情報} + \text{移転制御情報} \\ &\rightarrow \text{PAT} \langle \text{AID}_A \mid \text{AID}_{B1}, \text{AID}_{B2}, \dots, \\ &\quad \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \end{aligned}$$

(3) 分割 (Split PAT) (図35参照) :

ALISTを同一所有者AIDの複数ALISTに分解し、分解後のすべてのALISTに対し、それぞれ、有効期限情報および移転制御情報を設定する。

【数17】

$$\begin{aligned} &\text{ALIST} \langle \text{AID}_A \mid \text{AID}_{B1}, \text{AID}_{B2}, \dots, \\ &\quad \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle + \text{Enabler}_A \\ &\rightarrow \text{ALIST} \langle \text{AID}_A \mid \text{AID}_{B1}, \text{AID}_{B2}, \dots \rangle \\ &\quad + \text{ALIST} \langle \text{AID}_A \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\text{ALIST} \langle \text{AID}_A \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\quad + \text{Enabler of AID}_A + \text{有効期限情報} + \text{移転制御情報} \\ &\rightarrow \text{PAT} \langle \text{AID}_A \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \end{aligned}$$

(4) 所有者変更 (Trans PAT) (図36参照) :

ALITSの所有者AIDを変更し、変更後のALISTに対し有効期限情報および移転制御情報を設定する。

【0236】

【数18】

$$\begin{aligned} &\text{ALIST} \langle \text{AID}_A \mid \text{AID}_B \rangle \\ &\quad + \text{ALIST} \langle \text{AID}_A \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\quad + \text{Enabler of AID}_A + \text{Enabler of AID}_B \\ &\rightarrow \text{ALIST} \langle \text{AID}_B \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\text{ALIST} \langle \text{AID}_B \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \\ &\quad + \text{Enabler of AID}_B + \text{有効期限情報} + \text{移転制御情報} \\ &\rightarrow \text{PAT} \langle \text{AID}_B \mid \text{AID}_{C1}, \text{AID}_{C2}, \dots \rangle \end{aligned}$$

有効期限情報の設定における操作では、所有者AIDとこれに対応したEnablerの両者を所有するユーザにのみ有効期限情報の設定を許可するために、以下の操作を定義する。

【0237】

【数19】

$$\text{ALIST} < \text{AID}_A \mid \text{AID}_B > + \text{Enabler of } A + \text{有効期限情報} \\ \rightarrow \text{PAT} < \text{AID}_A \mid \text{AID}_B >$$

移転制御情報の設定における操作では、所有者AIDとこれに対応したEnablerの両者を所有するユーザにのみ移転制御情報の設定を許可するために、以下の操作を定義する。

【0238】

【数20】

$$\text{ALIST} < \text{AID}_A \mid \text{AID}_B > + \text{Enabler of } A + \text{移転制御情報} \\ \rightarrow \text{PAT} < \text{AID}_A \mid \text{AID}_B >$$

次に、本実施形態の全体構成を示す図37～図43について説明する。図37～図43において、通信網からAID_Aを割り当てられたユーザAは、ユーザAの計算機にAID_AおよびEnabler of AID_Aを保存し、フロッピードライブ、CD-ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_AおよびEnabler of AID_Aを保存している。

【0239】

同様に、通信網からAID_Bを割り当てられたユーザBは、自らの計算機にAID_BおよびEnabler of AID_Bを保存し、フロッピードライブ、CD-ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_AおよびEnabler of AID_Aを保存している。

【0240】

以下、ユーザAがPAT<AID_A | AID_B>を生成する手順を説明する。

【0241】

(1) ユーザAは、以下の手段のいずれかを用いて、 AID_B および $Enabler\ of\ AID_B$ を取得する。

- ・オンライン検索サービスに AID_B と $Enabler\ of\ AID_B$ を登録し、ユーザAが検索結果として取得するのを待つ(図37)。

- ・電子メール、シグナリング等で AID_B と $Enabler\ of\ AID_B$ をユーザAに直接送信する(図38～図39)。

- ・フロッピーディスク、CD-ROM、MO、ICカード等の磁気、光、電子メディアに AID_B と $Enabler\ of\ AID_B$ を蓄積し、ユーザAに渡す。または、ユーザAが閲覧して取得するのを待つ(図40～図41)。

- ・書籍、名刺等の紙メディアに AID_B と $Enabler\ of\ AID_B$ を記載し、ユーザAに渡す(図42～図43)。もしくは、ユーザAが閲覧し取得するのを待つ。

【0242】

(2) 上述した(1)のいずれかの手段で AID_B および $Enabler\ of\ AID_B$ を取得したユーザAは、PAT演算装置に対しMakePAT命令を発行する。この手順は図37～図43で共通で、以下の通りに定義する。

- (a) ユーザAは、ユーザAの通信端末に AID_A 、 $Enabler\ of\ AID_A$ 、 AID_B 、 $Enabler\ of\ AID_B$ 、有効期限情報、および移転制御情報値をセットし、MakePAT命令(図50)の発行を要求する。

- (b) ユーザAの通信端末は、MakePAT命令を生成する。

- (c) ユーザAの通信端末は、生成したMakePAT命令を電子メール、シグナリング等の手段でPAT演算装置に送信する(MakePAT命令の発行)。

【0243】

- (d) PAT演算装置は、受信したMakePAT命令を図44、図46、図47、図51に従って処理し、 $PAT<AID_A\ | AID_B>$ を生成する。具体的には、

【数21】

$$AID_A + AID_B + Enabler\ of\ AID_B + Enabler\ of\ AID_A$$

→ALIST<AID_A | AID_B>
 ALIST<AID_A | AID_B>+ Enabler of AID_A
 +有効期限情報+移転制御情報
 →PAT<AID_A | AID_B>

(e) PAT演算装置は、生成したPAT<AID_A | AID_B>を電子メール、シグナリング等の手段でユーザAの通信端末、または必要に応じて、ユーザBの通信端末に送信する。

【0244】

(f) ユーザA（またはユーザB）の通信端末は、受信したPAT<AID_A | AID_B>をユーザAの通信端末の記憶装置に保存する。

【0245】

PATのマージ（Merge PAT、図44、図46、図48、図52）、PATの分割（Split PAT、図45、図46、図49、図53）、PATの所有者変更（Trans PAT、図44、図46、図50、図54）も同様の手順である。

【0246】

次に、MakePAT、Merge PAT、Trans PATの処理の全体の流れを図44に従って説明する。

【0247】

1. 新規生成または変更後のPATの所有者AIDを決定する（ステップS4411）。
2. 新規生成または変更後のPATの会員AIDを決定する（ステップS4412）。
3. ステップS4411の所有者AIDとステップS4412の会員AIDを要素に持つAIDリストを生成する（ステップS4413）。

【0248】

4. メッセージから有効期限情報および移転制御情報を抽出する（ステップS4414）。

【0249】

5. ステップS4413のAIDリストに、ステップS4414の有効期限情報

および移転制御情報を設定する（ステップS4415）。

6. ステップS4415の結果に所有者インデックスを設定する（ステップS4416）。

7. ステップS4416の結果にPAT演算装置の識別子（シリアルナンバー）を設定する（ステップS4417）。

【0250】

8. ステップS4417の結果にPAT演算装置の識別子（シリアルナンバー）の秘密鍵で署名する（ステップS4418）。

【0251】

9. ステップS4418の結果を所有者AID宛に送信し、必要に応じて会員AID宛にも送信する（ステップS4419）。

【0252】

Split PATは、MakePAT、Merge PAT、Trans PATとは異なり、複数のPATを生成する。従って、Split PATの処理は図45に示すように図44の処理に再帰制御（ステップS4420）を加えることと定義する。

【0253】

次に、所有者AIDの決定について説明する。新規生成PATまたは内容変更後PATの所有者AIDの決定は、以下の手順に従う。

【0254】

MakePATの場合、所有者AIDの決定は、図47に示すように行われる。

【0255】

1. 図56のメッセージから、新規生成PATの所有者AIDにしたいAIDを抽出する（ステップS4711）。

2. 上記AIDが存在する場合には、上記メッセージから、新規生成PATの所有者AIDにしたいAIDのEnablerを抽出する（ステップS4712, S4713）。

【0256】

3. Enablerが存在する場合には、ステップS4711で抽出したAIDについて、ステップS4713で抽出したEnablerと対応しているか調べる（ステップ

S4714, S4715)。

4. 対応している場合には、抽出したAIDを新規生成PATの所有者AIDに決定し、対応していない場合には、処理を中止する(ステップS4716, S4717)。

Merge PATの場合、所有者AIDの決定は、図48に示すように行われる。

【0257】

1. 図57のメッセージから、マージ対象のPATをすべて抽出する(ステップS4811)。

2. ステップS4811で抽出したすべてのPATから、所有者AIDを抽出する(ステップS4812)。

3. ステップS4812で抽出した所有者AIDを比較し(ステップS4813)、少なくとも1個の所有者AIDが一致しない場合、処理を中止し、すべての所有者AIDが一致する場合、下記処理(ステップS4814)を実行する。

【0258】

4. 図57のメッセージから、マージ後PATの所有者AIDにしたいAIDのEnablerを抽出する(ステップS4814)。

5. Enablerが存在する場合、ステップS4813で比較の結果のAIDがステップS4814で抽出したEnablerと対応しているか調べ(ステップS4815, S4816)、対応している場合、ステップS4811で抽出したAIDをマージ後PATの所有者AIDに決定し、対応していない場合、処理を中止する(ステップS4817, S4818)。

【0259】

Split PATの場合、所有者AIDの決定は、図49に示すように行われる。

【0260】

1. 図58のメッセージから、分割対象のPATを抽出する(ステップS4911)。

2. ステップS4911で抽出したPATから、所有者AIDを抽出する(ステップS4912)。

3. 図58のメッセージから、分割後のすべてのPATの所有者AIDにしたい

A I DのEnabler を抽出する（ステップS4913）。

【0261】

4. Enabler が存在する場合、ステップS4912で抽出したA I DがステップS4913で抽出したEnabler と対応しているか調べ（ステップS4914, S4915, S4916）、対応している場合、ステップS4911で抽出したA I Dを分割後のすべてのP A Tの所有者A I Dに決定し（ステップS4917）、対応していない場合、処理を中止する（ステップS4916）。

【0262】

Trans P A Tの場合、所有者A I Dの決定は、図50に示すように行われる。

【0263】

1. 図59のメッセージから、変更対象のP A Tを抽出する（ステップS5011）。
2. この抽出したP A Tから、（現在の）所有者A I Dを抽出する（ステップS5012）。
3. 図59のメッセージから、（現在の）所有者A I DのEnabler を抽出する（ステップS5013）。

【0264】

4. Enabler が存在する場合、ステップS5012で抽出したA I DがステップS5013で抽出したEnabler と対応しているか調べる（ステップS5014～S5016）。
5. 対応している場合、図59のメッセージから、新しく所有者A I DにしたいA I Dを抽出し、対応していない場合は処理を中止する（ステップS5017）。
6. 上記A I Dが会員A I Dである場合、上記メッセージから、新しく所有者A I DにしたいA I DのEnabler を抽出する（ステップS5018, S5019）。

【0265】

7. Enabler が存在する場合、ステップS5017で抽出したA I DがステップS5019で抽出したEnabler と対応しているか調べ（ステップS5020～S

5022)、対応している場合ステップS5017で抽出したAIDを新所有者AIDに決定し(ステップS5023)、対応していない場合、処理を中止する(ステップS5022)。

【0266】

次に、会員AIDの決定について説明する。新規生成PATまたは内容変更後PATの会員AIDの決定は、以下の手順に従う。

【0267】

MakePATの場合、所有者AIDの決定は、図51に示すように行われる。

【0268】

1. 図56のメッセージから、新規生成PATの会員AIDにしたいAIDをすべて抽出する(ステップS5111)。
2. AIDが存在する場合には、図56のメッセージから、新規生成PATの会員AIDにしたいすべてのAIDについて、それぞれEnablerを抽出する(ステップS5112, S5113)。

【0269】

3. Enablerが存在する場合、ステップS5111で抽出したすべてのAIDについて、それぞれステップS5112で抽出したEnablerと対応しているか調べ(ステップS5114~S5116)、対応しているAIDを新規生成PATの会員AIDに決定し(ステップS5117)、対応していないAIDを廃棄し、すべての処理対象AIDについて上記処理を繰り返し行う(ステップS5118)。

【0270】

MergePATの場合、会員AIDの決定は、図52に示すように行われる。

【0271】

1. 図57のメッセージから、マージ対象のすべてのPATを抽出する(ステップS5211)。
2. この抽出したすべてのPATから、それぞれ(所有者インデックスをもとに)所有者AIDを抽出する(ステップS5212)。
3. この抽出したすべての所有者AIDをマージ後の所有者AIDに決定したA

IDと比較する（ステップS5213）。

【0272】

4. 一致する場合には、PATから会員AIDを抽出し（ステップS5214）、この抽出した会員AIDをマージ後の会員AIDに追加する（ステップS5215）。

【0273】

5. 一致しない場合、PATを削除し、処理対象を次のPATとして、上記処理を繰り返し行い、処理対象が存在しない場合には、処理を中止する（ステップS5216）。

【0274】

Split PATの場合、会員AIDの決定は、図53に示すように行われる。

【0275】

1. 図58のメッセージから分割対象のPATを抽出する（ステップS5311）。

2. この抽出したPATから所有者AIDを抽出する（ステップS5312）。

3. この抽出した所有者AIDを分割後の所有者AIDに決定したAIDと比較する（ステップS5313）。

【0276】

4. 一致する場合には、メッセージから会員AIDのリストを抽出し（ステップS5314）、一致しない場合には、処理を中止する。

5. ステップS5311のPATから、ステップS5314のリストに含まれる会員AIDをすべて抽出する（ステップS5315）。

6. この抽出した会員AIDの組み合わせを分割後の会員AIDに決定する（ステップS5316）。

【0277】

Trans PATの場合、会員AIDの決定は、図54に示すように行われる。

【0278】

1. 図59のメッセージから所有者変更したいPATを抽出し、この抽出したPATからすべての会員AIDを抽出する（ステップS5411）。

2. 所有者AIDを変更後PATの会員AIDにするかチェック（ステップS5412）、会員AIDにする場合には、ステップS5411のPATから所有者AIDも抽出する（ステップS5413）。

3. ステップS5413のAIDを変更後PATの会員AIDに決定する（ステップS5414）。

【0279】

次に、AIDリストの生成について説明する。AIDリストの生成は、MakePAT、MergePAT、SplitPAT、TransPATで共通であり、図46に示すように行われる。

【0280】

1. 会員AID数をもとに、AIDリストのバッファ長を決定する（ステップS4611）。

2. この決定した情報をもとに、バッファを生成する（ステップS4612）。

3. 所有者AIDをステップS4612のバッファの空き領域にコピーする（ステップS4613）。

4. 会員AIDをステップS4613の残りの空き領域にコピーする（ステップS4614）。

5. 次の会員AIDが存在する場合には、ステップS4614に戻り、繰り返す（ステップS4615）。

【0281】

次に、Enablerの正当性の検証について説明する。このEnablerの正当性の検証は、MakePAT、MergePAT、SplitPAT、TransPATで共通であり、図55に示すように行われる。

【0282】

1. AIDとEnablerを入力する（ステップS5511）。

2. この入力されたAIDとEnabler中のAIDをCA公開鍵で認証する（ステップS5512）。改竄されている場合には、処理を中止する（ステップS5513）。

3. Enablerであることを証明する文字列を入力する（ステップS5514）。

【0283】

4. ステップS5511のEnabler の先頭フィールドとステップS5514の文字列を比較する（ステップS5515）。一致しない場合には、処理を中止する（ステップS5516）。
5. 一致する場合には、ステップS5511のAIDとEnabler 中のAIDを比較する（ステップS5517, S5518）。
6. 比較処理結果（一致した or 一致しなかった）を出力する（ステップS5519）。

【0284】

次に、上述した実施形態を一元管理型メーリングリストに適用した例について図60を参照して説明する。コンピュータネットワーク上のグループ通信にメーリングリストがある。以下、メーリングリストにおける連絡先情報管理への適用例を説明する。

【0285】

一般に、メーリングリストにおける連絡先リスト（会員のメールアドレスから構成されるリストであり、以後、会員リストと呼ぶ）は、主催者がアクセス可能なインターネット上のサーバ（または、パソコン通信のホスト）において一元的に管理されている（インターネット上のサーバとしては、listserverが広く利用されている）。

【0286】

サーバ（ホスト）の主な仕事は：

- (1) メーリングリストへの入会申請者から入会届を受信したら、入会申請者のメールアドレスを会員リストに追加する、
 - (2) メーリングリストからの退会申請者から退会届を受信したら、退会申請者のメールアドレスを会員リストから削除する、
- の2点である。

【0287】

入会届、退会届の書式は、一般に、入会希望、退会希望を定型化した命令、もしくはこれらを意味する自然言語（例えば「入会したい」という意味を持つ日本

語文字列)と、入会申請者、退会申請者のメールアドレスから構成される。例えば、listserverの場合には、

(1) 入会届

subscribe メーリングリスト名 自分のメールアドレス

(2) 退会届

unsubscribe メーリングリスト名 自分のメールアドレス

とインターネットメールの本文に記述する。

【0288】

まず、入会処理について説明する。図60において、オンライン検索サービスは、ADS同様、検索時に検索者AIDと検索者AIDのEnablerを送信すると、検索者に対しPAT<検索者AID | 登録者AID>を通知する。以下、入会処理の流れを説明する。

【0289】

1. 主催者AID登録：主催者は、主催者AID、Enabler of 主催者AID、申請用の有効期限情報、申請用の移転制御情報、および公開情報をオンライン検索サービスに登録する。

【0290】

2. 入会申請用PAT発行：申請者が検索条件、申請者AID、およびEnabler of 申請者AIDを送信すると、オンライン検索サービスは以下の手順に従いPAT<申請者AID | 主催者AID>を発行する。

【0291】

(1) オンライン検索サービスは以下のMakePAT命令を生成し、PAT演算装置に送信する。

MakePAT

申請者AID Enabler of 申請者AID

主催者AID Enabler of 主催者AID

申請用の有効期限情報

申請用の移転制御情報

(2) PAT演算装置は、受信したMakePAT命令を解釈し、PAT<主催者A

ID | 申請者AID>を生成する。具体的には、

【数22】

申請者AID+主催者AID+ Enabler of 主催者AID
 + Enabler of 申請者AID
 →ALIST<主催者AID | 申請者AID>
 ALIST<申請者AID | 主催者AID>
 + Enabler of 申請者AID+申請用の有効期限情報
 + 申請用の移転制御情報
 →PAT<申請者AID | 主催者AID>

(3) PAT演算装置は、生成したPAT<申請者AID | 主催者AID>をオンライン検索サービスに送信する。

【0292】

(4) PAT<申請者AID | 主催者AID>を受信したオンライン検索サービスは、このPATを検索結果として申請者に送信する。

【0293】

3. 入会申請：入会申請者は、入会申請の旨とPAT<申請者AID | 主催者AID>、申請者AID、Enabler of 申請者を主催者に送信する。

【0294】

4. 会員登録：申請者AIDを会員リストPAT<主催者AID | 既会員AID>に登録するまでの流れを以下に説明する。

【0295】

(1) 主催者は、以下のTrans PAT命令を生成してPAT演算装置に送信する。

【0296】

Trans PAT
 PAT<申請者AID | 主催者AID>
 申請者AID Enabler of 申請者AID
 主催者AID Enabler of 主催者AID
 任意の（テンポラリな）有効期限情報

任意の（テンポラリな）移転制御情報

(2) 上記Trans PAT命令を受信したPAT演算装置は、PAT<主催者AID | 申請者AID>を生成し、このPATを主催者に送信する。具体的には、
【数23】

ALIST<申請者AID | 主催者AID>
+ Enabler of 申請者AID + Enabler of 主催者AID
→ALIST<主催者AID | 申請者AID>
ALIST<主催者AID | 申請者AID> + Enabler of 主催者AID
+ 任意の有効期限情報 + 任意の移転制御情報
→PAT<主催者AID | 申請者AID>

(3) PAT演算装置は、生成したPAT<主催者AID | 申請者AID>を主催者に送信する。

【0297】

(4) 主催者は、PAT<主催者AID | 申請者AID>を受信したら、以下のMerge PAT命令を生成してPAT演算装置に送信する。

【0298】

Merge PAT
PAT<主催者AID | 既会員AID>
PAT<主催者AID | 申請者AID>
Enabler of 主催者AID
正式な有効期限情報
正式な移転制御情報

(5) 上記Merge PAT命令を受信したPAT演算装置は、PAT<主催者AID | 既会員AID、申請者AID>を生成する。具体的には、
【数24】

ALIST<主催者AID | 既会員AID>
+ ALIST<主催者AID + 申請者AID>
+ Enabler of 主催者AID
→ALIST<主催者AID | 既会員AID、申請者AID>

ALIST<主催者AID | 既会員AID、申請者AID>

+ Enabler of 主催者AID+会員リストの正式な有効期限情報

+会員リストの正式な移転制御情報

→PAT<主催者AID | 既会員AID、申請者AID>

(6) PAT演算装置は、生成したPAT<主催者AID | 既会員AID、申請者AID>を主催者に送信する。

【0299】

5. 通知：主催者は、PAT<主催者AID | 既会員AID、申請者AID>を申請者に電子メールで送信する。

【0300】

退会処理は、上記した3. 入会申請～5. 通知と同様の流れで行われる。

【0301】

なお、オンライン検索サービス以外で主催者AIDが提供された場合、すなわちフロッピーディスク、CD-ROM、紙メディア等で主催者AIDが提供された場合には、入会申請者は、図38～図43のいずれかの手順でPAT<申請者AID | 主催者AID>を生成する。以後は、上述した3. 入会申請～5. 通知と同様の流れで行う。

【0302】

次に、図61～図64を参照して、本発明の第3の実施形態について説明する。

【0303】

上述した実施形態における個別化アクセスチケット（PAT）の新規生成（MakePAT）およびマージ（MergePAT）では、会員AIDとEnabler of 会員AIDを個別化アクセスチケットの所有者に渡すことが必要であるが、これを所有者に渡すと、その所有者が別の所有者の主催するグループ通信に対して、取得した会員AIDで参加することが可能になる。すなわち、会員AIDを用いた成りすましが可能になるという問題がある。また、その所有者が取得した会員AIDおよびEnabler of 会員AIDを不特定多数が閲覧可能なメディアに掲載すれば、誰でもその会員AIDにアクセス可能になるため、会員AIDのユーザへの

嫌がらせが発生する恐れがあるとともに、また第三者による会員AIDを用いた成りすましも可能になるという問題がある。

【0304】

そこで、本実施形態では、Enabler of 会員AIDを所有者AIDに渡さなくとも、MakePATおよびMergePATを可能にする。

【0305】

このために、本実施形態では、Null-AID (AID_{Null}) および該Null-AIDの Enabler(Enabler of Null-AIDまたは Enabler of AID_{Null}) を使用して、個別化アクセスチケット (PAT) の新規生成および既存の個別化アクセスチケット (PAT) の内容変更を行うものである。ここで、Null-AIDを含む演算は、以下のすべての規則に従う：

- (a) 上述した実施形態における新規生成 (MakePAT)、マージ (MergePAT)、分割 (SplitPAT)、変更 (TransPAT) からなる演算規則、
- (b) Null-AIDにのみ適用可能な規則として、
 - i. Null-AIDは、すべてのユーザに既知であり、
 - ii. Enabler of Null-AIDは、すべてのユーザに既知である。

【0306】

ここで、上述した実施形態で定義した演算規則について説明する。

【0307】

- (1) 複数AIDからPATを作る (MakePAT) :

【数25】

$$\begin{aligned} & \text{AID}_{\text{所有者}} + \text{AID}_{\text{会員1}} + \text{AID}_{\text{会員2}} +, \dots, + \text{AID}_{\text{会員N}} \\ & + \text{Enabler of AID}_{\text{会員1}} + \text{Enabler of AID}_{\text{会員2}} +, \dots, \\ & + \text{Enabler of AID}_{\text{会員N}} + \text{Enabler of AID}_{\text{所有者}} \\ \rightarrow & \text{PAT} \langle \text{AID}_{\text{所有者}} | \text{AID}_{\text{会員1}}, \text{AID}_{\text{会員2}}, \dots, \text{AID}_{\text{会員N}} \rangle \end{aligned}$$

- (2) 同一所有者の複数PATをマージする (MergePAT) :

【数26】

$$\begin{aligned} & \text{PAT} \langle \text{AID}_{\text{所有者}} | \text{AID}_{\text{会員a1}}, \text{AID}_{\text{会員a2}}, \dots, \text{AID}_{\text{会員aN}} \rangle \\ & + \text{PAT} \langle \text{AID}_{\text{所有者}} | \text{AID}_{\text{会員b1}}, \text{AID}_{\text{会員b2}}, \dots, \end{aligned}$$

AID_{会員bN}>
 + Enabler of AID_{所有者}
 →PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, ..., AID_{会員aM},
 AID_{会員b1}, AID_{会員b2}, ..., AID_{会員bN}>

(3) PATを同一所有者の複数PATに分割する (Split PAT) :

【数27】

PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, ..., AID_{会員aM},
 AID_{会員b1}, AID_{会員b2}, ..., AID_{会員bN}>
 + Enabler of AID_{所有者}
 →PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, ...,
 AID_{会員aM}>
 + PAT<AID_{所有者} | AID_{会員b1}, AID_{会員b2}, ...,
 AID_{会員bN}>

(4) PATの所有者AIDを変更する (Trans PAT) :

【数28】

PAT<AID_{所有者} | AID_{会員a1}, AID_{会員a2}, ..., AID_{会員aM}>
 + PAT<AID_{所有者} | AID_{新所有者}>
 + Enabler of AID_{所有者} + Enabler of AID_{新所有者}
 →PAT<AID_{新所有者} | AID_{会員a1}, AID_{会員a2}, ...,
 AID_{会員aM}>

次に、Null-AIDに関する演算例について説明する：

(1) AID_A と Enabler of AID_A とからPAT<AID_{Null} | AID_A>
 を作る場合：

(a) Null-AIDの規則1(b)i. および1(b)ii.より、AID_{Null}と E
 nabler of AID_{Null}は既知である。

【0308】

(b) MakePATにより

【数29】

AID_{Null} + AID_A + Enabler of AID_A + Enabler of AID_{Null}

→PAT<AID_{Null} | AID_A>

(2) PAT<AID_{Null} | AID_A>とPAT<AID_{Null} | AID_B>とからPAT<AID_{Null} | AID_A, AID_B>を作る場合:

(a) Null-AIDの規則1(b)i. および1(b)ii.より、AID_{Null}とEnabler of AID_{Null}は既知である。

【0309】

(b) Merge PATにより

【数30】

PAT<AID_{Null} | AID_A>+PAT<AID_{Null} | AID_B>
+ Enabler of AID_{Null}

→PAT<AID_{Null} | AID_A, AID_B>

(3) PAT<AID_{Null} | AID_A>とPAT<AID_{Null} | AID_B>とEnabler of AID_AとからPAT<AID_A | AID_B>を作る場合:

(a) Null-AIDの規則1(b)i. および1(b)ii.より、AID_{Null}とEnabler of AID_{Null}は既知である。

【0310】

(b) Trans PATにより

【数31】

PAT<AID_{Null} | AID_A>+PAT<AID_{Null} | AID_B>
+ Enabler of AID_{Null}+ Enabler of AID_A

→PAT<AID_A | AID_B>

Null-AIDのデータ構造は、図61に示すように、Null-AIDであることを一意に表す文字列(例えば、この文字列の値は認証局CAで定義される)および該文字列に対して認証局CAの署名を施したもので構成される。

【0311】

また、Enabler of Null-AIDのデータ構造は、図62に示すように、Enablerであることを一意に表す文字列(例えば、この文字列は認証局CAで定義される)、Null-AIDの実体、および前記Enablerであることを表す文字列と前記Null-AIDの実体を連結した文字列に対して認証局CAの署名

を施したもので構成される。

【0312】

なお、Null-AIDおよび Enabler of Null-AIDは、セキュアなPAT演算装置およびセキュアなPAT認証局で保持される。

【0313】

次に、本実施形態の第1の応用例について図63を参照して説明する。図63において、

(1) ユーザB (PAT会員) は、ユーザBの端末と接続されたセキュアなPAT演算装置で前記Null-AIDに関する演算例(1)を実行して $PAT\langle AID_{Null} | AID_B \rangle$ を生成し、任意の手段でユーザA (PAT所有者) に渡す。

【0314】

(2) $PAT\langle AID_{Null} | AID_B \rangle$ を受信したユーザAは、ユーザAの端末に接続されたセキュアなPAT演算装置で

(a) Null-AIDに関する演算例(1)を実行して $PAT\langle AID_{Null} | AID_A \rangle$ を作る。

【0315】

(b) Null-AIDに関する演算例(3)を実行して $PAT\langle AID_A | AID_B \rangle$ を作る。

【0316】

(3) ユーザAは、生成した $PAT\langle AID_A | AID_B \rangle$ を任意の手段でユーザAに渡す。

【0317】

なお、有効期限の決定方法は前述した方法と共通のため省略する。また、Null-AIDに関する演算の処理は前述した方法と共通のため省略する。

【0318】

$PAT\langle AID_{Null} | AID_A, AID_B \rangle$ をユーザBに渡す場合には、上述した演算(2)において、前記Null-AIDに関する演算例(2)を実行する。

【0319】

次に、本実施形態の第2の応用例について図64を参照して説明する。図64において、

(1) ユーザB (PAT会員) は、ユーザBの端末と接続されたセキュアなPAT演算装置でNull-AIDに関する演算例(1)を実行して $PAT < AID_{Null} | AID_B >$ を作り、任意の公開情報とともにオンライン検索サービス(データベース)に登録する。

【0320】

(2) ユーザA (PAT所有者) は、ユーザAの端末に接続されたセキュアなPAT演算装置でユーザBの端末と接続されたセキュアなPAT演算装置でNull-AIDに関する演算例(1)を実行して $PAT < AID_{Null} | AID_A >$ を作り、任意の検索条件とともにオンライン検索サービスに提示する。

【0321】

(3) ユーザBの個人情報がユーザAの提示した検索条件を満足した場合、オンライン検索サービスに接続されたセキュアなPAT演算装置は

(a) Null-AIDに関する演算例(2)を実行して $PAT < AID_{Null} | AID_A, AID_B >$ を作る。

【0322】

(b) $PAT < AID_{Null} | AID_A, AID_B >$ をオンライン検索サービスに渡す。

【0323】

(1) オンライン検索サービスは、PAT演算装置で作られた $PAT < AID_{Null} | AID_A, AID_B >$ をユーザAに渡す。

【0324】

(2) $PAT < AID_{Null} | AID_A, AID_B >$ を受け取ったユーザAは、ユーザAの端末に接続されたセキュアなPAT演算装置で下記のTrans PAT演算を実行して、 $PAT < AID_A | AID_B >$ を作る。

【0325】

【数32】

$$\begin{aligned} &PAT<AID_{Null} | AID_A > \\ &+ PAT<AID_{Null} | AID_A, AID_B > \\ &+ Enabler\ of\ AID_{Null} + Enabler\ of\ AID_A \\ \rightarrow &PAT<AID_A | AID_B > \end{aligned}$$

尚、有効期限の決定方法は前述した方法と共通のため省略する。また、Null-AIDに関する演算の処理は前述した方法と共通のため省略する。

【0326】

$PAT<AID_A | AID_B >$ をオンライン検索サービスに接続されたセキュアなPAT演算装置で生成する場合には、そのPAT演算装置に Enabler of AID_A を渡す。そして、上述した演算(3)において、Null-AIDに関する演算例(3)を実行する。

【0327】

$PAT<AID_B | AID_A >$ をオンライン検索サービスに接続されたセキュアなPAT演算装置で生成して、ユーザBに渡す場合には、そのPAT演算装置に Enabler of AID_B を渡す。そして、上述した演算(3)において、Null-AIDに関する演算例(3)と同様の演算を実行する。

【0328】

次に、本発明の第4の実施形態について図65～図68を参照して説明する。

【0329】

グループ通信においては参加者を固定したい状況はしばしば発生するが、上述した実施形態では個別化アクセスチケット(PAT)を変更不可にする機能を持たないため、参加者を固定することができない。すなわち、上述した実施形態では、参加者を固定するか否かは、個別化アクセスチケットの所有者の判断に一任されている。

【0330】

そこで、本実施形態では、個別化アクセスチケットに読取専用属性を設定している。

【0331】

このため、本実施形態では、God-AID (AID_{God}) を用いて、個別化アクセスチケット (PAT) に読取専用属性を設定している。ここで、God-AIDに関する演算は、以下のすべての規則に従う：

- (a) God-AIDは、すべてのユーザに既知であり、
- (b) God-AIDに関する演算は、以下のいずれかのみ許可される：

【数33】

i. $AID_{所有者}$ が AID_{Null} でも AID_{God} でもない場合：

$$\begin{aligned} & PAT < AID_{所有者} | AID_{会員1}, AID_{会員2}, \\ & \quad \dots, AID_{会員N} > \\ & + \text{Enabler of } AID_{所有者} \\ & \rightarrow PAT < AID_{God} | AID_{所有者}, AID_{会員1}, AID_{会員2}, \\ & \quad \dots, AID_{会員N} > \end{aligned}$$

ii. $AID_{所有者}$ が AID_{Null} の場合：

$$\begin{aligned} & PAT < AID_{Null} | AID_{会員1}, AID_{会員2}, \\ & \quad \dots, AID_{会員N} > \\ & + \text{Enabler of } AID_{Null} \\ & \rightarrow PAT < AID_{God} | AID_{会員1}, AID_{会員2}, \\ & \quad \dots, AID_{会員N} > \end{aligned}$$

God-AIDのデータ構造は、図65に示すように、God-AIDであることを一意に表す文字列（例えば、この文字列の値は認証局CAで定義される）および該文字列に対して認証局CAの署名を施したものから構成される。God-AIDは、上述したセキュアなPAT演算装置およびセキュアなPAT認証局で保持されている。

【0332】

God-AID規則の処理について図66に示すフローチャートを参照して説明する。図66において、

1. 個別化アクセスチケットの所有者AIDと、Null-AIDとGod-AIDを入力する（ステップS6611）。

【0333】

2. ステップS6611で入力した所有者AIDとGod-AIDを文字列比較する(ステップS6613)。

【0334】

・完全に一致するか否かをチェック(ステップS6615)、完全に一致する場合には、処理を中止するが、一部でも一致しなかった場合には、次のステップS6617に進む。

【0335】

3. 上記所有者AIDをステップS6611で入力したNull-AIDと文字列比較する(ステップS6617)。

【0336】

(a) 完全に一致するか否かをチェックし(ステップS6619)、完全に一致する場合には、

i. Enabler of Null-AIDを入力する(ステップS6621)。

【0337】

ii. 上記所有者AID(すなわち、Null-AID)とステップS6621で入力したEnabler of Null-AIDを用いて、Enabler of Null-AIDの正当性を判定する(ステップS6623)(尚、判定手順は図55に従う)。

【0338】

・Enabler of Null-AIDがNull-AIDの正当なEnablerである場合(ステップS6623)、所有者AID(すなわち、Null-AID)をGod-AIDで上書きしてから、終了する(ステップS6625)。

【0339】

・Enabler of Null-AIDがNull-AIDの正当なEnablerでない場合には、処理を中止する。

【0340】

(b) ステップS6619の判定において、一部でも一致しない場合、

i. Enabler of 所有者AIDを入力する(ステップS6627)。

【0341】

ii. 上記所有者AIDとステップS6627で入力した Enabler of 所有者AIDを用いて、Enabler of 所有者AIDの正当性を判定する（判定手順は図55に従う）（ステップS6629）。

【0342】

・ Enabler of 所有者AIDが所有者AIDの正当なEnabler である場合（ステップS6631）、ステップS6633へ進む。

【0343】

・ Enabler of 所有者AIDが所有者AIDの正当なEnabler でない場合（ステップS6631）、処理を中止する。

【0344】

iii. God-AIDを個別化アクセスチケットPATに連結する（ステップS6633）。

【0345】

iv. 個別化アクセスチケットPATの所有者Index をGod-AIDに設定する（ステップS6635）。

【0346】

次に、本実施形態の応用例について図67を参照して説明する。

【0347】

$PAT\langle AID_{Null} | AID_A \rangle$ と $PAT\langle AID_{Null} | AID_B \rangle$ とから $PAT\langle AID_{God} | AID_A, AID_B \rangle$ を作る場合、PAT所有者（図67におけるユーザA）の端末に接続されたセキュアなPAT演算装置において、以下の演算を実行する。

【0348】

(1) 上述した新規生成の演算規則Merge PATにより

【数34】

$$\begin{aligned} & PAT\langle AID_{Null} | AID_A \rangle + PAT\langle AID_{Null} | AID_B \rangle \\ & + \text{Enabler of } AID_{Null} \\ \rightarrow & PAT\langle AID_{Null} | AID_A, AID_B \rangle \end{aligned}$$

(2) God-AIDに関する演算規則(a)より、AID_{God}は既知である。

【0349】

(3) God-AIDに関する演算規則(b)ii.より

【数35】

$PAT \langle AID_{Null} | AID_A, AID_B \rangle$

+ Enabler of AID_{Null}

$\rightarrow PAT \langle AID_{God} | AID_A, AID_B \rangle$

上記演算は、第三者の計算機（サーチエンジンなど）に接続されたセキュアなPAT演算装置（図68）またはセキュアな認証局でも実行される。

【0350】

次に、図69を参照して、本発明の第5の実施形態について説明する。

【0351】

上述した第3の実施形態で説明したように、Null-AIDを追加すると、以下に説明するように、個別化アクセスチケット（PAT）の所有者（所有者AIDのユーザ）が会員（会員AIDのユーザ）へのアクセス権を第三者に委譲できるようになるという問題がある。しかも、会員に無断で委譲可能である。

【0352】

1. $PAT \langle AID_A | AID_B \rangle$ の所有者Aが（会員はB）

・ $PAT \langle AID_A | AID_B \rangle$

・ AID_A

・ Enabler of AID_A

を用いて、 $PAT \langle AID_{Null} | AID_B \rangle$ を作る。ここで、Aは、 $PAT \langle AID_A | AID_B \rangle$ に加えて

・ AID_A

・ Enabler of AID_A

・ AID_{Null}

・ Enabler of AID_{Null}

をすべて知っているとする。

【0353】

(a) Aは、MakePATにより、 $PAT\langle AID_A \mid AID_{Null} \rangle$ を作る。

【0354】

【数36】

$AID_A + AID_{Null} + \text{Enabler of } AID_{Null} + \text{Enabler of } AID_A$
 $\rightarrow PAT\langle AID_A \mid AID_{Null} \rangle$

(b) Aは、Trans PATにより、 $PAT\langle AID_{Null} \mid AID_B \rangle$ を作る。

【0355】

【数37】

$PAT\langle AID_A \mid AID_B \rangle + PAT\langle AID_A \mid AID_{Null} \rangle$
 $+ \text{Enabler of } AID_A + \text{Enabler of } AID_{Null}$
 $\rightarrow PAT\langle AID_{Null} \mid AID_B \rangle$

上記1(b)の後、Aが $PAT\langle AID_{Null} \mid AID_{\text{会員}} \rangle$ を第三者Cに渡すと

【0356】

2. Cは、 $PAT\langle AID_{Null} \mid AID_B \rangle$ を用いて、 $PAT\langle AID_C \mid AID_B \rangle$ を作る。ここで、Cは、 $PAT\langle AID_{Null} \mid AID_{\text{会員}} \rangle$ に加えて

- ・ AID_C
- ・ $\text{Enabler of } AID_C$
- ・ AID_{Null}
- ・ $\text{Enabler of } AID_{Null}$

をすべて知っているとする。

【0357】

(a) Cは、MakePATにより、 $PAT\langle AID_{Null} \mid AID_C \rangle$ を作る。

【0358】

【数38】

$AID_{Null} + AID_C + \text{Enabler of } AID_{Null} + \text{Enabler of } AID_C$
 $\rightarrow PAT\langle AID_{Null} \mid AID_C \rangle$

(b) Cは、Trans PATにより、 $PAT\langle AID_C \mid AID_B \rangle$ を作る。

【0359】

【数39】

$$\begin{aligned} & PAT<AID_{Null} | AID_B> + PAT<AID_{Null} | AID_C> \\ & + \text{Enabler of } AID_{Null} + \text{Enabler of } AID_C \\ & \rightarrow PAT<AID_C | AID_B> \end{aligned}$$

上記2(b)の結果、Cは $PAT<AID_C | AID_B>$ を得るので、Bへのアクセスが可能になる。

【0360】

そこで、本実施形態では、 $PAT<AID_{所有者} | AID_{会員}>$ の所有者が $AID_{会員}$ のEnablerを知らない場合には、このPATから $PAT<AID_{Null} | AID_{会員}>$ を作ることができないようにする。

【0361】

このため、本実施形態では、PATの所有者が $AID_{会員}$ のEnablerなしで $PAT<AID_{Null} | AID_{会員}>$ を作るためには、 $PAT<AID_{所有者} | AID_{Null}>$ を作ることが必要になる。

【0362】

そこで、上述した第3の実施形態で説明したNull-AIDに対して、以下の規則を追加する。

【0363】

Null-AIDはPATの所有者AIDとしてのみ使用できる（会員AIDとしては使用できない）。

【0364】

・ $PAT<AID_{Null} | AID_{会員1}, AID_{会員2}, \dots, AID_{会員N}>$ は許可する。

【0365】

・ $PAT<AID_{所有者} | AID_{Null}, AID_{会員1}, AID_{会員2}, \dots, AID_{会員N}>$ は許可しない。

【0366】

上述した実施形態におけるセキュアなPAT演算装置とセキュアなPAT認証

局にそれぞれNull-AIDが会員AIDに含まれているか否かをチェックする機能を追加する。この会員AIDのチェック処理機能について図69に示すフローチャートを参照して説明する。図69において、

1. Null-AIDとPATを入力する（ステップS6911）。

【0367】

2. ステップS6911で入力したPATから、会員AIDをすべて抽出する（ステップS6913）。

【0368】

3. この抽出したすべての会員AIDについて、それぞれ、ステップS6911で入力したNull-AIDと文字列比較する（ステップS6915）。

【0369】

・すべての会員AIDがNull-AIDと完全に一致しない場合（ステップS6917、S6919）、Merge PAT、Split PAT、またはTrans PAT処理に移る（図44または図45）（ステップS6921）。

【0370】

・会員AIDが1つでもNull-AIDと完全に一致する場合（ステップS6917）、処理を中止する。

【0371】

次に、図70～図80を参照して、本発明の第6の実施形態について説明する。この第6の実施形態は、上述した第1の実施形態において図3に示した役割識別子AIDに対して後述する図71（b）のようにリンク情報を追加するとともに、図3に示した1対1個別化アクセスチケットPATに含まれていた役割識別子AIDの実体の代わりに前記役割識別子AIDのリンク情報を図71（c）に示すように設定し、該リンク情報で役割識別子AIDを一意に特定するように構成した点が異なるものである。

【0372】

なお、このようにリンク情報を追加された役割識別子AIDをリンク情報付き役割識別子AIDと称し、AIDのリンク情報を有する1対1個別化アクセスチケットPATをリンク指定型1対1個別化アクセスチケットPATと称すること

にする。また、リンク情報は、役割識別子AIDを一意に特定可能な情報であり、認証局CAによって役割識別子AIDに対して一意に付与されるシリアル番号である。

【0373】

まず、図70を参照して、本発明の第6の実施形態の全体構成図について説明する。図70において、1は認証局CAであり、認証権限と役割識別子AIDの発行権限を有し、ユーザに対して役割識別子を割り当てる機能を有する。3はユーザあり、5はセキュア・コミュニケーション・サービスSCSであり、ユーザ3間の電子メールを転送し、必要に応じて着信拒否および個人識別子の同一性を判定し、取り出す。7はアノニマス・ディレクトリ・サービスADSであり、役割識別子AID、移転制御情報、有効期限、および、プライバシー情報を管理するデータベースである。すなわち、アノニマス・ディレクトリ・サービスADS7は、検索者の役割識別子AIDと検索条件（一般に、プライバシー情報）にマッチした登録者の役割識別子AIDから個別化アクセスチケットPATを発行し、検索者に交付する機能を有する。

【0374】

ユーザの要求に基づいて個人識別子から役割識別子AIDを生成し、そのユーザに割り当てるまでの一連の処理はリンク情報が付加されることを除いて第1の実施形態と基本的に同じであるが、具体的に図71を参照して説明する。

【0375】

図71は、個人識別子OID(Official Identification)とリンク情報付き役割識別子AIDの例を示している。同図に示すように、個人識別子OIDは、図71(a)に示すように認証局CA1がユーザに一意に生成した任意の文字列に対して認証局CA1が秘密鍵で電子署名したものである。また、リンク情報付き役割識別子AIDは、図71(b)に示すように個人識別子OIDの一部とその位置情報、冗長な文字列、SCSのホストOID、およびリンク情報からなる文字列に対し、認証局CA1の秘密鍵で電子署名を施したものである。

【0376】

また、リンク指定型1対1個別化アクセスチケットPATは、図71(c)に

示すように、発信者フラグ、移転制御フラグ、役割識別子 AID_0 のリンク情報、役割識別子 AID_1 のリンク情報、有効期限からなる文字列に対してアノニマス・ディレクトリ・サービスADSのOID秘密鍵による電子署名を施したものである。

【0377】

ユーザ3がリンク情報付き役割識別子AIDを認証局CA1に対して請求する処理は、図4に示したフローチャートを参照した上述した説明と同じである。

【0378】

次に、上述した役割識別子AIDの請求に対する認証局CA1が役割識別子AIDをユーザ3に対して交付する処理も図5に示すフローチャートを参照した説明と同じである。

【0379】

ユーザにおけるAID交付処理も図6を参照した説明と同じである。

【0380】

次に、認証局CAにおける役割識別子AIDの生成処理について図72、図73を参照して説明する。図72において、認証局CA1は乱数発生等の任意の手段を用いて、個人識別子OIDの全長Lと等しい長さの文字列を生成し、この文字列を仮の役割識別子AIDとして生成する（ステップS911）。

【0381】

次に、個人識別子OIDの複写を行うために、個人識別子OIDのコピー範囲を指定するpとlの値を決定する（ステップS913）。これは、乱数発生等の任意の手段を用いて、パラメータ p_i と l_i の値をそれぞれ $0 \leq p_i \leq L$ および $l_{\min} \leq l_i \leq l_{\max}$ のようにコピー範囲を決定する。ここで、Lは個人識別子OIDの全長であり、 l_{\min} および l_{\max} は $0 < l_{\min} < l_{\max} < L$ が成り立つ範囲で任意に定めた値とする。それから、コピー先頭位置を個人識別子OIDの先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにコピー範囲を設定する。次に、図73（a）、（b）に示すように、ペースト先頭位置を仮の役割識別子AIDの先頭から距離 p_i に設定し、終端位置を $p_i + l_i$ に設定するというようにペースト位置を設定する。

【0382】

それから、図73(a)，(b)に示すように、上述したコピー範囲の文字列を仮の役割識別子AIDの上述したペースト位置に上書きして複写する(ステップS915)。このように上書きした文字列の特定の位置に位置情報 p_i および l_i の値を、CAが定めた方法で暗号化して、図73(c)で指定した位置に付加し(ステップS917)、更にこの位置情報を付加した文字列にセキュア・コミュニケーション・サービスSCSのホストOID(ホスト名、ドメイン名、またはIPアドレス)を図73(c)に示すように付加し(ステップS919)、更に図73(c)に示すようにリンク情報を付加する(ステップS920)。そして、このようにセキュア・コミュニケーション・サービスSCSのホストOIDおよびリンク情報を付加した文字列に認証局CAのOID秘密鍵で電子署名を施す(ステップS921)。

【0383】

次に、役割識別子AIDによる個人情報の登録および検索について説明する。アノニマス・ディレクトリ・サービスADS7において、個人情報を登録するまでの流れを図74(a)に示すが、この処理は図11(a)で行ったものと同じである。

【0384】

また、アノニマス・ディレクトリ・サービスADS7における検索処理は、図74(b)に示すように、検索者であるユーザAが、自らの役割識別子AIDと例えば性別、年齢、趣味といったプライバシー情報からなる検索条件をアノニマス・ディレクトリ・サービスADS7に送信する。アノニマス・ディレクトリ・サービスADS7は、これらの情報を受信すると、検索条件にマッチした登録者の役割識別子AIDを抽出する。アノニマス・ディレクトリ・サービスADS7は最後に検索者の役割識別子AIDと検索条件にマッチした登録者の役割識別子AIDのそれぞれのリンク情報から個別化アクセスチケットPATを生成し、検索者であるユーザA3に交付する。

【0385】

個別化アクセスチケットの生成は、アノニマス・ディレクトリ・サービスAD

S7の検索結果として生成する。

【0386】

次に、図75のフローチャートを参照して、ADSにおけるPAT生成処理について説明する。この図75に示すPAT生成処理は、図12で説明した処理においてステップS1215における処理を図75のステップS1216で示すようにステップS1211で認証済みの検索者AIDのリンク情報を、登録者AID（ADS登録時に登録者AIDの秘密鍵で認証済み）のリンク情報と連結するというように変更した点が異なるのみでその他の処理は同じである。なお、このステップS1216で連結した検索者AIDのリンク情報と登録者AIDのリンク情報からなる文字列に、登録者によりあらかじめ設定された移動制御フラグと有効期限を設定し、更に発信者フラグを「0」と設定する（ステップS1217）。

【0387】

次に、リンク指定型1対1個別化アクセスチケットPATによる移転制御について説明する。移転制御は、発信者番号通知のために行われるが、この発信者番号通知とは、着信者が発信者の役割識別子AIDと実際の発信者を対応付けられるようにすることである。

【0388】

アノニマス・ディレクトリ・サービスADS7および着信者は、個別化アクセスチケットPATの移転制御フラグを設定することにより、発信者に番号通知させるか否かを選択させることができる。

【0389】

移転制御フラグを「1」に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われるため、着信者は発信者の役割識別子AIDと実際の発信者を対応付けることができる（発信者番号通知）。また、移転制御フラグを「0」に設定した場合には、着信者は発信者の役割識別子AIDと実際の発信者を対応付けることができない（発信者番号非通知）。

【0390】

図77のフローチャートを参照して、SCSにおけるメール接続制御の処理手

順について説明する。この処理は図14のステップS1419, S1421の処理における発信者AIDを図77のステップS1420, S1422にそれぞれ示すように発信者AIDのリンク情報に変更する点異なるのみであり、その他の処理は同じである。

【0391】

1. メールを入力する(ステップS1411)。

【0392】

2. ステップS1411で入力したメールのTo:フィールドからPATを抽出する。次に、このPATに対するADS公開鍵をADSに何らかの手段で問い合わせ、そのADS公開鍵を取得する。そして、PATをADS公開鍵で認証する(ステップS1413)。

【0393】

3. ステップS1413における認証の結果

- ・PATが改竄されている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する(ステップS1429)。

【0394】

- ・PATが改竄されていない場合、ステップS1417に進む。

【0395】

4. ステップS1411のメールのFrom:フィールドから発信者AIDを抽出する。また、メールのTo:フィールドのPATの移転制御フラグを解析し、PATから発信者AIDのリンク情報を抽出する(ステップS1417, S1420)。

【0396】

5. ステップS1417, S1420で抽出した発信者AIDのリンク情報同士を比較する(ステップS1422)。

【0397】

6. ステップS1422における比較の結果

- ・両者が一致しない場合ステップS1411のメールを、メールのFrom:

フィールドに記述された発信者AID宛に返信して、処理を中止する（ステップS1429）。

【0398】

・両者が一致する場合、ステップS1425に進む。

【0399】

7. ステップS1411のメールのTo:フィールドのPATから有効期限を抽出する（ステップS1425）。

【0400】

8. ステップS1411のメールのTo:フィールドのPATが有効期限内かどうかを検証する（ステップS1427）。

【0401】

9. ステップS1427における検証の結果

・有効期限を過ぎている場合、ステップS1411のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する（ステップS1429）。

【0402】

・有効期限内の場合、ステップS1431に進む。

【0403】

10. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を調べる。

【0404】

11. ステップS1411のメールのTo:フィールドのPATから移転制御フラグ値を抽出する（ステップS1431）。

【0405】

12. ステップS1431における抽出の結果

・移転制御フラグ値が「1」の場合、図15～図17の手順に従い、移転制御を行ってから（ステップS1435）、図78の手順に従い、メールを着信者AID宛に転送する（ステップS1437）。

【0406】

・移転制御フラグ値が「0」の場合、図78の手順に従い、メールを着信者AID宛に転送する（ステップS1437）。

【0407】

移転制御は、図15～図17を参照して説明したとおりである。

【0408】

次に、図78のフローチャートを参照して接続制御について説明する。この接続制御は、図18の処理においてステップS1811を図78のステップS1810のように変更し、図18のステップS1811とS1813の間に図78のステップS1851、S1853を追加したものである。

【0409】

1. メールのTo:フィールドのPATから、発信者AIDのリンク情報と着信者AIDのリンク情報を抽出する（ステップS1810）。この抽出したリンク情報をすべてCAに提示して、発信者AIDと着信者AIDを取得し（ステップS1851）、この取得したすべてのAIDから、SCSホストOIDを抽出する（ステップS1853）。

【0410】

2. この抽出した発信者、着信者それぞれのSCSホストOIDのデータ形式を調べる（ステップS1813）。

【0411】

3. ステップS1813における調査の結果

・発信者SCSホストOIDと着信者SCSホストOIDのうち、少なくとも一方がホスト名もしくはドメイン名で与えられている場合には、ステップS1815に進み、ホスト名またはドメイン名で与えられているSCSホストOIDをDNS(Domain Name Service)に問い合わせ、そのホスト名またはドメイン名に対するIPアドレスを取得してから、ステップS1817に進む。

【0412】

・発信者SCSホストOIDと着信者SCSホストOIDがともにIPアドレスで与えられている場合には、そのままステップS1817に進む。

【0413】

4. ステップS1815, S1817で抽出あるいは変換したIPアドレスを比較する(ステップS1817)。

【0414】

5. ステップS1817における比較の結果

・発信者SCSホストOID(IPアドレス)と着信者SCSホストOID(IPアドレス)が一致する場合、ステップS1819からステップS1823に進み、発信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する(ステップS1823)。この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1825からステップS1827に進み、ステップS1810のメールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0415】

また、ステップS1825において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、着信者AIDを検索条件として、着信拒否データベースに問い合わせる(ステップS1829)。

【0416】

この問い合わせの結果、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1831からステップS1827に進み、メールを、メールのFrom:フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0417】

また、ステップS1831において、メールのTo:フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されていない場合、メールを、着信者のメールボックスまたはスプールに格納して正常終了する(ステップS1833)。

【0418】

一方、ステップS1819において、発信者SCSホストOID（IPアドレス）と着信者SCSホストOID（IPアドレス）が一致しない場合について説明する。

【0419】

まず、SMTPに従い、メールを着信者AIDをアカウントに持つSCSホストに転送する（ステップS1835）。

【0420】

次に、着信者AIDをアカウントに持つSCSホスト上で、着信者AIDを検索する（ステップS1837）。

【0421】

この検索の結果、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在しない場合、ステップS1839からステップS1841に進み、メールを、メールのFrom：フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0422】

また、ステップS1839において、着信者AIDのアカウントが、発信者AIDをアカウントに持つSCSホスト上に存在する場合、ステップS1843に進む。ステップS1843では着信者AIDを検索条件として、着信拒否データベースに問い合わせる。

【0423】

ステップS1843における問い合わせの結果、メールのTo：フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登録されている場合、ステップS1845からステップS1841に進み、メールを、メールのFrom：フィールドに記述された発信者AID宛に返信して、処理を中止する。

【0424】

また、ステップS1845において、メールのTo：フィールドのPAT、または、発信者AIDに含まれるSCSホストOIDが着信拒否データベースに登

録されていない場合、ステップS1847に進み、メールを、着信者のメールボックスまたはスプールに格納して正常終了する。

【0425】

SCSにおけるメール返信処理は、図19で説明した処理と同じである。

【0426】

次に、個別化アクセスチケットPATに対する着信拒否について説明する。着信者AID側で指定した個別化アクセスチケットPATがTo:フィールドに記述されたメールが、着信者AIDに含まれるホストOIDのセキュア・コミュニケーション・サービスSCS5に到着した場合には、そのセキュア・コミュニケーション・サービスSCS5はそのメールを着信者のメールボックスまたはスプールには格納せず、発信者AID宛に返信する。この一連の処理を着信拒否と呼ぶ。

【0427】

ユーザにおける着信拒否申請処理は、図22に示すフローチャートを参照した説明と同じである。

【0428】

セキュア・コミュニケーション・サービスSCS5における着信拒否設定処理は、図23を参照した説明と同じである。

【0429】

図79のフローチャートおよび図80を参照して、同一性の判定について説明する。

【0430】

1. 変数OID_Mの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する。また、変数OID_Vの初期値を、OIDの全長Lと等しい長さで、かつ、すべての値が0であるビット列と定義する（ステップS2511）。

【0431】

2. 処理対象のAIDの集合から1個のAIDを選択し、以下のビット演算を実行する（ステップS2513）。

【0432】

(a) AIDに含まれる位置情報をもとにして、変数AID_Mと変数AID_Vの値を決定する(ステップS2515)。ここで、

- ・ AID_M はOIDの全長Lと等しい長さで、かつ、
- －OID情報が定義されている位置の値は1である。

【0433】

- －OID情報が定義されていない位置の値は0である。

【0434】

ビット列と定義する(図80)。

【0435】

- ・ AID_V はOIDの全長Lと等しい長さで、かつ、
 - －OID情報が定義されている位置の値はOID情報の実際の値である
 - －OID情報が定義されていない位置の値は0である
- ビット列と定義する(図80)。

【0436】

(b) OID_MとAID_MのAND演算を実行し、その結果を変数OVR_Mに代入する(ステップS2517)。

【0437】

(c) OVR_MとAID_MのAND演算と、OVR_MとOID_MのAND演算を実行し、その演算結果を比較する(ステップS2519)。

【0438】

・一致する場合OID_MとAID_MのOR演算を実行し、実行結果をOID_Mに代入する(ステップS2521)。また、OID_VとAID_VのOR演算を実行し、実行結果をOID_Mに代入する(ステップS2523)。

【0439】

- ・一致しない場合、ステップS2525に進み、実行する。

【0440】

(d) 処理対象のAIDの集合から、次に処理するAIDを抽出する。

【0441】

・集合に少なくとも1個のAIDが含まれている場合、ステップS2519を実行する。

【0442】

・集合にAIDが1個も含まれていない場合、ステップS2527に進む。

【0443】

(e) OID_M および OID_V の値を出力する（ステップS2527）。

【0444】

最終的に得られた OID_M の値は、処理対象のAIDの集合から復元できたOID情報のすべての位置を表している。また、最終的に得られた OID_V の値は、処理対象のAIDの集合から復元できたOID情報のすべてを表している。つまり、 OID_M と OID_V の値を用いると、

(a) OID_V の値を検索条件とすると、確率的にはあるがOIDを求めることができる。

【0445】

(b) 上記検索の精度を、OID全長Lとの比 OID_M/L で定量的に評価することができる。

【0446】

上述したように、本実施形態では、ユーザは、氏名、電話番号、電子メールアドレスといった情報を含む個人識別子OIDからこれらの情報を隠蔽した役割識別子AIDを作成すべく役割識別子AID請求メッセージを作成し、認証局CA1に送信すると、認証局CA1は、該メッセージを受け取って、リンク情報付き役割識別子AIDを生成し、ユーザに交付する。

【0447】

ユーザは、この交付されたリンク情報付き役割識別子AIDおよび性別、年齢、趣味等の個人情報をアノニマス・ディレクトリ・サービスADS7に送信し、アノニマス・ディレクトリ・サービスADS7にリンク情報付き役割識別子AIDと個人情報を登録する。このように登録された情報を検索する場合は、検索者は自己のリンク情報付き役割識別子AIDと検索条件（性別、年齢、趣味等のプ

ライバシー情報)をアノニマス・ディレクトリ・サービスADS7に送信する。アノニマス・ディレクトリ・サービスADS7は、これらの情報を受信すると、該検索条件にマッチした登録者のリンク情報付き役割識別子AIDを抽出する。そして、アノニマス・ディレクトリ・サービスADS7は、検索者のリンク情報付き役割識別子AIDと検索条件にマッチした登録者のリンク情報付き役割識別子AIDからリンク指定型1対1個別化アクセスチケットPATを生成し、検索者に交付する。

【0448】

このリンク指定型1対1個別化アクセスチケットPATには、図71(c)に示すように発信者フラグ、移転制御フラグ、有効期限の値が設定されるが、この有効期限を着信者側で設定することにより、発信者からの接続を制限することができる。

【0449】

また、移転制御フラグの設定内容により発信者に番号通知させるか否かを、すなわち着信者が発信者AIDと実際の発信者を対応づけられるようにすることができるか否かを選択することができる。すなわち、移転制御フラグを1に設定した場合には、セキュア・コミュニケーション・サービスSCS5で移転制御が行われ、着信者は発信者AIDと実際の発信者を対応付けることができる(発信者番号通知)。また、該フラグを0に設定した場合は、移転制御は行われず、着信者は発信者AIDと実際の発信者を対応付けることはできない(発信者番号非通知)。

【0450】

また、リンク指定型1対1個別化アクセスチケットPATで着信者を指定した呼をリンク指定型1対1個別化アクセスチケットPATのリンク情報で特定した着信者役割識別子AIDまたは発信者役割識別子AIDに着信するように、通信網に対して接続要求をすることができる。更に、リンク指定型1対1個別化アクセスチケットPATで指定した呼のうち、着信者が選択したリンク指定型1対1個別化アクセスチケットPATの呼を着信拒否することができる。また更に、匿名性を悪用し複数の発信者役割識別子AIDで個人攻撃を繰り返す発信者への対

処として、それら複数の発信者役割識別子A I Dから個人識別子O I Dの同一性を判定することができ、かつ、その個人識別子のある確率で取り出すことができる。

【0451】

次に、本発明の第7の実施形態に係る接続制御方法について図81乃至図101を参照して説明する。上述した第6の実施形態では発信者と着信者を1対1に対応させるとともに、偽装防止のためにユーザ要求に基づいたリンク指定型1対1個別化アクセスチケットの新規生成、内容変更を許可していない場合について説明したのに対して、第7の実施形態では、上述した第2の実施形態と同様に、発信者と着信者を1対Nに対応させるとともに、リンク指定型1対N個別化アクセスチケットの新規生成、内容変更をユーザ主導で可能とする場合について説明するものである。なお、この発信者および着信者は所有者または会員である。

【0452】

第2の実施形態で説明したと同様に、グループ通信（メーリングリスト等）の会員構成は動的に変化するため、グループ通信の主催者は会員の電話番号、電子メールアドレス、インターネットメールアドレス等の連絡先情報を管理する必要がある。これに対して、第6の実施形態のように、リンク指定型1対1個別化アクセスチケットの新規生成、内容変更ができない場合には、連絡先情報の管理が困難である。例えば、グループを一体として管理することが困難であり、また移転制御のため、他の人に渡しても、メーリングリスト等グループ通信のアドレスとして機能しない。

【0453】

本第7の実施形態では、このような不具合を解消するためにリンク指定型1対N個別化アクセスチケットP A Tの新規生成および既存のリンク指定型1対N個別化アクセスチケットP A Tの内容変更をユーザ主導でできるようにしている。

【0454】

まず、本第7の実施形態で使用される各識別子の定義について図81、図82を参照して説明する。

【0455】

個人識別子 (Official Identification : O I D) は、図81 (a) に示すように、認証局 (Certificate Authority : C A) が任意に生成した文字列 (電話番号、電子メールアドレス等)、または前記文字列に対し C A 秘密鍵で電子署名を施したものである。

【0456】

リンク情報付き役割識別子 (Anonymous Identification : A I D) は、図81 (b) に示すように、O I D の一部分とその位置情報、任意に生成した冗長な文字列、S C S のホスト O I D、およびリンク情報からなる文字列に対し、C A 秘密鍵で電子署名を施したものである。また、A I D は S C S や C A で暗号化する場合もある。なお、リンク情報は、第6の実施形態のものと同一である。

【0457】

リンク指定型1対N個別化アクセスチケット (Personalized Access Ticket : P A T) は、図81 (c) に示すように、1個の所有者 A I D (Holder A I D) のリンク情報、1個以上の会員 A I D (Member A I D) のリンク情報、発信者インデックス、所有者インデックス、有効期限情報、移転制御情報、P A T 演算装置識別子から構成されるリストに対し、P A T 演算装置識別子の秘密鍵で署名したものである。ここで、発信者インデックスは、A I D のリンク情報のリスト中の発信者 A I D のリンク情報の位置を表す数値データで、先頭 A I D が発信者 A I D であれば1、2番目ならば2、…、n番目ならばnである。所有者インデックスは、A I D のリンク情報のリスト中の所有者 A I D のリンク情報の位置を表す数値データで、先頭 A I D が所有者 A I D であれば1、2番目ならば2、…、n番目ならばnであると定義する。移転制御情報は、移転可の場合は「0」という数値、また移転不可の場合は「1」という数値のいずれかで表す。

【0458】

所有者 A I D のリンク情報は、A I D リンク情報リスト中の所有者インデックスで指定した位置に書き込まれている A I D リンク情報である。会員 A I D のリンク情報は、所有者 A I D リンク情報以外のすべての A I D リンク情報である。有効期限情報は、数値データであって、使用可能回数、P A T が利用不可能にな

る絶対時刻（UTC）、PATが利用可能になる絶対時刻（UTC）、PATが利用可能になってから利用不可能になるまでの相対時間（寿命）のいずれか、または複数を組み合わせて記述する。PAT演算装置識別子は、PAT演算装置のシリアルナンバーである。PAT演算装置の秘密鍵は、上記シリアルナンバーに対する秘密鍵である。これらの中で、所有者AIDリンク情報と会員AIDリンク情報からなる部分を以後、AIDリストと呼ぶことにする。

【0459】

また、本第7の実施形態では、所有者役割識別子AIDに対応した識別子として、Enablerを導入している。Enablerは、図82に示すように、Enablerであることを通信網上で一意に表す文字列とAIDからなる文字列に対して、CA秘密鍵で電子署名したものである。

【0460】

次にPATの新規生成および内容変更における操作について説明する。通信端末上のセキュアなPAT演算装置、CA上もしくはCAから正当に依頼されたネットワーク上のPAT演算オブジェクト（以後、これもPAT演算装置と呼ぶことにする）において、次の操作が定義されるが、これは第2の実施形態のものと同じであり、図33～図36を参照して説明する。

【0461】

(1) AIDリストの演算：

所有者AIDおよび所有者AIDに対応するEnablerを用いて、AIDリストを新規生成あるいは変更する。

【0462】

(2) 有効期限情報および移転制御情報の設定：

所有者AIDおよび所有者AIDに対応するEnablerを用いて、有効期限情報および移転制御情報を設定もしくは変更する。

【0463】

所有者AIDに対してのみAIDリストの演算を許可するために、以下の演算規則を定義する。

【0464】

(1) 新規生成 (MakePAT) (図33参照) :

AIDリスト (ALIST<所有者AID | 会員AID₁, 会員AID₂,
..., 会員AID_n>) を新規生成し、生成後のALISTに対し、有効期限情報
および移転制御情報を設定する。

【0465】

【数40】

$$\begin{aligned} & \text{AID}_A + \text{AID}_B + \text{Enabler of AID}_B + \text{Enabler of AID}_A \\ \rightarrow & \text{ALIST} < \text{AID}_A | \text{AID}_B > \text{ALIST} < \text{AID}_A | \text{AID}_B > \\ & + \text{Enabler of AID}_A + \text{有効期限情報} + \text{移転制御情報} \\ \rightarrow & \text{PAT} < \text{AID}_A | \text{AID}_B > \end{aligned}$$

(2) マージ (MergePAT) (図34参照) :

同一所有者AIDの複数ALISTをマージし、マージ後のALISTに対し、有効期限情報および移転制御情報を設定する。

【0466】

【数41】

$$\begin{aligned} & \text{ALIST} < \text{AID}_A | \text{AID}_{B1}, \text{AID}_{B2}, \dots > \\ & + \text{ALIST} < \text{AID}_A | \text{AID}_{C1}, \text{AID}_{C2}, \dots > \\ & + \text{Enabler of AID}_A \\ \rightarrow & \text{ALIST} < \text{AID}_A | \text{AID}_{B1}, \text{AID}_{B2}, \dots, \\ & \text{AID}_{C1}, \text{AID}_{C2}, \dots > \\ & \text{ALIST} < \text{AID}_A | \text{AID}_{B1}, \text{AID}_{B2}, \dots, \text{AID}_{C1}, \text{AID}_{C2}, \dots > \\ & + \text{Enabler of AID}_A + \text{有効期限情報} + \text{移転制御情報} \\ \rightarrow & \text{PAT} < \text{AID}_A | \text{AID}_{B1}, \text{AID}_{B2}, \dots, \\ & \text{AID}_{C1}, \text{AID}_{C2}, \dots > \end{aligned}$$

(3) 分割 (SplitPAT) (図35参照) :

ALISTを同一所有者AIDの複数ALISTに分解し、分解後のすべてのALISTに対し、それぞれ、有効期限情報および移転制御情報を設定する。

【数42】

$$\begin{aligned}
 &ALIST<AID_A | AID_{B1}, AID_{B2}, \dots, \\
 &\quad AID_{C1}, AID_{C2}, \dots> + Enabler_A \\
 \rightarrow &ALIST<AID_A | AID_{B1}, AID_{B2}, \dots> \\
 &\quad + ALIST<AID_A | AID_{C1}, AID_{C2}, \dots> \\
 &ALIST<AID_A | AID_{C1}, AID_{C2}, \dots> \\
 &\quad + Enabler \text{ of } AID_A + \text{有効期限情報} + \text{移転制御情報} \\
 \rightarrow &PAT<AID_A | AID_{C1}, AID_{C2}, \dots>
 \end{aligned}$$

(4) 所有者変更 (Trans PAT) (図36参照) :

ALITSの所有者AIDを変更し、変更後のALISTに対し有効期限情報および移転制御情報を設定する。

【0467】

【数43】

$$\begin{aligned}
 &ALIST<AID_A | AID_B > \\
 &\quad + ALIST<AID_A | AID_{C1}, AID_{C2}, \dots> \\
 &\quad + Enabler \text{ of } AID_A + Enabler \text{ of } AID_B \\
 \rightarrow &ALIST<AID_B | AID_{C1}, AID_{C2}, \dots> \\
 &ALIST<AID_B | AID_{C1}, AID_{C2}, \dots> \\
 &\quad + Enabler \text{ of } AID_B + \text{有効期限情報} + \text{移転制御情報} \\
 \rightarrow &PAT<AID_B | AID_{C1}, AID_{C2}, \dots>
 \end{aligned}$$

有効期限情報の設定における操作では、所有者AIDとこれに対応したEnablerの両者を所有するユーザにのみ有効期限情報の設定を許可するために、以下の操作を定義する。

【0468】

【数44】

$$\begin{aligned}
 &ALIST<AID_A | AID_B > + Enabler \text{ of } A + \text{有効期限情報} \\
 \rightarrow &PAT<AID_A | AID_B >
 \end{aligned}$$

移転制御情報の設定における操作では、所有者AIDとこれに対応したEnablerの両者を所有するユーザにのみ移転制御情報の設定を許可するために、以下の操作を定義する。

【0469】

【数45】

ALIST<AID_A | AID_B>+ Enabler of A+移転制御情報
→PAT<AID_A | AID_B>

次に、本実施形態の全体構成を示す図83～図89について説明する。図83～図89において、通信網からAID_Aを割り当てられたユーザAは、ユーザAの計算機にAID_AおよびEnabler of AID_Aを保存し、フロッピードライブ、CD-ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_AおよびEnabler of AID_Aを保存している。

【0470】

同様に、通信網からAID_Bを割り当てられたユーザBは、自らの計算機にAID_BおよびEnabler of AID_Bを保存し、フロッピードライブ、CD-ROMドライブ、通信ボード、マイクロフォン、スピーカー等の入出力機器を接続している。または、上記仕様と同等の機能を持つ通信端末（電話、携帯電話等）に、AID_AおよびEnabler of AID_Aを保存している。

【0471】

以下、ユーザAがPAT<リンク(AID_A) | リンク(AID_B)>を生成する手順を説明する。

【0472】

(1) ユーザAは、以下の手段のいずれかを用いて、AID_BおよびEnabler of AID_Bを取得する。

【0473】

・オンライン検索サービスにAID_BとEnabler of AID_Bを登録し、ユーザAが検索結果として取得するのを待つ（図83）。

【0474】

・電子メール、シグナリング等でAID_BとEnabler of AID_BをユーザAに直接送信する（図84～図85）。

【0475】

・フロッピーディスク、CD-ROM、MO、ICカード等の磁気、光、電子メディアに AID_B と $Enabler\ of\ AID_B$ を蓄積し、ユーザAに渡す。または、ユーザAが閲覧して取得するのを待つ（図86～図87）。

【0476】

・書籍、名刺等の紙メディアに AID_B と $Enabler\ of\ AID_B$ を記載し、ユーザAに渡す（図88～図89）。もしくは、ユーザAが閲覧し取得するのを待つ。

【0477】

(2) 上述した(1)のいずれかの手段で AID_B および $Enabler\ of\ AID_B$ を取得したユーザAは、PAT演算装置に対しMakePAT命令を発行する。この手順は図83～図89で共通で、以下の通りに定義する。

【0478】

(a) ユーザAは、ユーザAの通信端末に AID_A 、 $Enabler\ of\ AID_A$ 、 AID_B 、 $Enabler\ of\ AID_B$ 、有効期限情報、および移転制御情報値をセットし、MakePAT命令の発行を要求する。

【0479】

(b) ユーザAの通信端末は、MakePAT命令を生成する。

【0480】

(c) ユーザAの通信端末は、生成したMakePAT命令を電子メール、シグナリング等の手段でPAT演算装置に送信する（MakePAT命令の発行）。

【0481】

(d) PAT演算装置は、受信したMakePAT命令を図44、図90、図91、図95に従って処理し、 $PAT<リンク(AID_A) | リンク(AID_B)>$ を生成する。具体的には、

【数46】

$$\begin{aligned} &AID_A + AID_B + Enabler\ of\ AID_B + Enabler\ of\ AID_A \\ &\quad \rightarrow ALIST<AID_A | AID_B> \\ &ALIST<AID_A | AID_B> + Enabler\ of\ AID_A \end{aligned}$$

+有効期限情報+移転制御情報

→PAT<リンク(AID_A) | リンク(AID_B)>

(e) PAT演算装置は、生成したPAT<リンク(AID_A) | リンク(AID_B)>を電子メール、シグナリング等の手段でユーザAの通信端末、または必要に応じて、ユーザBの通信端末に送信する。

【0482】

(f) ユーザA(またはユーザB)の通信端末は、受信したPAT<リンク(AID_A) | リンク(AID_B)>をユーザAの通信端末の記憶装置に保存する。

【0483】

PATのマージ(Merge PAT、図44、図90、図92、図96)、PATの分割(Split PAT、図45、図46、図49、図53)、PATの所有者変更(Trans PAT、図44、図90、図94、図98)も同様の手順である。

【0484】

次に、MakePAT、Merge PAT、Trans PATの処理の全体の流れを図44に従って説明する。

【0485】

1. 新規生成または変更後のPATの所有者AIDを決定する(ステップS4411)。

【0486】

2. 新規生成または変更後のPATの会員AIDを決定する(ステップS4412)。

【0487】

3. ステップS4411の所有者AIDとステップS4412の会員AIDを要素に持つAIDリストを生成する(ステップS4413)。

【0488】

4. メッセージから有効期限情報および移転制御情報を抽出する(ステップS4414)。

【0489】

5. ステップS4413のAIDリストに、ステップS4414の有効期限情報および移転制御情報を設定する（ステップS4415）。

【0490】

6. ステップS4415の結果に所有者インデックスを設定する（ステップS4416）。

【0491】

7. ステップS4416の結果にPAT演算装置の識別子（シリアルナンバー）を設定する（ステップS4417）。

【0492】

8. ステップS4417の結果にPAT演算装置の識別子（シリアルナンバー）の秘密鍵で署名する（ステップS4418）。

【0493】

9. ステップS4418の結果を所有者AID宛に送信し、必要に応じて会員AID宛にも送信する（ステップS4419）。

【0494】

Split PATは、MakePAT、Merge PAT、Trans PATとは異なり、複数のPATを生成する。従って、Split PATの処理は図45に示すように図44の処理に再帰制御（ステップS4420）を加えることと定義する。

【0495】

次に、所有者AIDの決定について説明する。新規生成PATまたは内容変更後PATの所有者AIDの決定は、以下の手順に従う。

【0496】

MakePATの場合、所有者AIDの決定は、図91に示すように行われる。

【0497】

1. 図56のメッセージから新規生成PATの所有者AIDにしたいAIDを抽出する（ステップS4711）。

【0498】

2. 上記AIDが存在する場合には、上記メッセージから、新規生成PATの所

有者AIDにしたいAIDのEnablerを抽出する（ステップS4712, S4713）。

【0499】

3. Enablerが存在する場合には、ステップS4711で抽出したAIDについて、ステップS4713で抽出したEnablerと対応しているか調べる（ステップS4714, S4715）。

【0500】

4. 対応している場合には、抽出したAIDのリンク情報を新規生成PATの所有者AIDのリンク情報に決定し、対応していない場合には、処理を中止する（ステップS4716, S4718）。

【0501】

Merge PATの場合、所有者AIDの決定は、図92に示すように行われる。

【0502】

1. 図99のメッセージから、マージ対象のPATをすべて抽出する（ステップS4811）。

【0503】

2. ステップS4811で抽出したすべてのPATから、所有者AIDのリンク情報を抽出する（ステップS4820）。このリンク情報をCAに提示して所有者AIDを取得する（ステップS4822）。

【0504】

3. ステップS4822で取得した所有者AIDを比較し（ステップS4813）、少なくとも1個の所有者AIDが一致しない場合、処理を中止し、すべての所有者AIDが一致する場合、下記処理（ステップS4814）を実行する。

【0505】

4. 図99のメッセージから、マージ後PATの所有者AIDにしたいAIDのEnablerを抽出する（ステップS4814）。

【0506】

5. Enablerが存在する場合、ステップS4813で比較の結果のAIDがステップS4814で抽出したEnablerと対応しているか調べ（ステップS4815）。

、S4816)、対応している場合、ステップS4811で抽出したAIDのリンク情報をマージ後PATの所有者AIDのリンク情報に決定し、対応していない場合、処理を中止する(ステップS4817、S4824)。

【0507】

Split PATの場合、所有者AIDの決定は、図93に示すように行われる。

【0508】

1. 図100のメッセージから、分割対象のPATを抽出する(ステップS4911)。

【0509】

2. ステップS4911で抽出したPATから、所有者AIDのリンク情報を抽出する(ステップS4921)。このリンク情報をCAに提示して、所有者AIDを取得する(ステップS4923)。

【0510】

3. 図100のメッセージから、分割後のすべてのPATの所有者AIDにしたAIDのEnablerを抽出する(ステップS4913)。

【0511】

4. Enablerが存在する場合、ステップS4923で取得したAIDがステップS4913で抽出したEnablerと対応しているか調べ(ステップS4914、S4915、S4916)、対応している場合、ステップS4911で抽出したAIDのリンク情報を分割後のすべてのPATの所有者AIDのリンク情報に決定し(ステップS4925)、対応していない場合、処理を中止する(ステップS4916)。

【0512】

Trans PATの場合、所有者AIDの決定は、図94に示すように行われる。

【0513】

1. 図101のメッセージから、変更対象のPATを抽出する(ステップS5011)。

2. この抽出したPATから、(現在の)所有者AIDのリンク情報を抽出する(ステップS5025)。このリンク情報をCAに提示して、(現在の)所有者

AIDを取得する(ステップS5027)。

【0514】

3. 図101のメッセージから、(現在の)所有者AIDのEnablerを抽出する(ステップS5013)。

4. Enablerが存在する場合、ステップS5012で抽出したAIDがステップS5013で抽出したEnablerと対応しているか調べる(ステップS5014～S5016)。

【0515】

5. 対応している場合、図101のメッセージから、新しく所有者AIDにしたいAIDを抽出し、対応していない場合は処理を中止する(ステップS5017)。

【0516】

6. 上記AIDが会員AIDである場合、上記メッセージから、新しく所有者AIDにしたいAIDのEnablerを抽出する(ステップS5018, S5019)。

【0517】

7. Enablerが存在する場合、ステップS5017で抽出したAIDがステップS5019で抽出したEnablerと対応しているか調べ(ステップS5020～S5022)、対応している場合ステップS5017で抽出したAIDのリンク情報を変更後PATの所有者AIDである新所有者AIDのリンク情報に決定し(ステップS5023)、対応していない場合、処理を中止する(ステップS5022)。

【0518】

次に、会員AIDの決定について説明する。新規生成PATまたは内容変更後PATの会員AIDの決定は、以下の手順に従う。

【0519】

MakePATの場合、所有者AIDの決定は、図51に示すように行われる。

【0520】

1. 図56のメッセージから、新規生成PATの会員AIDにしたいAIDをす

べて抽出する（ステップS5111）。

2. AIDが存在する場合には、図56のメッセージから、新規生成PATの会員AIDにしたいすべてのAIDについて、それぞれEnabler を抽出する（ステップS5112, S5113）。

【0521】

3. Enabler が存在する場合、ステップS5111で抽出したすべてのAIDについて、それぞれステップS5112で抽出したEnabler と対応しているか調べ（ステップS5114～S5116）、対応しているAIDのリンク情報を新規生成PATの会員AIDのリンク情報に決定し（ステップS5117）、対応していないAIDを廃棄し、すべての処理対象AIDについて上記処理を繰り返す（ステップS5118）。

【0522】

Merge PATの場合、会員AIDの決定は、図96に示すように行われる。

【0523】

1. 図99のメッセージから、マージ対象のすべてのPATを抽出する（ステップS5211）。

2. この抽出したすべてのPATから、それぞれ（所有者インデックスをもとに）所有者AIDのリンク情報を抽出する（ステップS5221）。

【0524】

3. この抽出したすべての所有者AIDのリンク情報をマージ後PATの所有者AIDのリンク情報と一致するか比較する（ステップS5223）。

【0525】

4. 一致する場合には、PATからすべての会員AIDのリンク情報を抽出し（ステップS5225）、この抽出した会員AIDのリンク情報をすべてマージ後の会員AIDのリンク情報に決定する（ステップS5227）。

【0526】

5. 一致しない場合、PATを削除し、処理対象を次のPATとして、上記処理を繰り返し行い、処理対象が存在しない場合には、処理を中止する（ステップS5216）。

【0527】

Split PATの場合、会員AIDの決定は、図97に示すように行われる。

【0528】

1. 図100のメッセージから分割対象のPATを抽出する（ステップS5311）。
2. この抽出したPATから所有者AIDのリンク情報を抽出する（ステップS5321）。

【0529】

3. この抽出したリンク情報を分割後PATの所有者AIDのリンク情報と一致するか比較する（ステップS5323）。

【0530】

4. 一致する場合には、メッセージから会員AIDのリストを抽出し（ステップS5314）、一致しない場合には、処理を中止する。

【0531】

5. ステップS5311のPATから、上記リストに含まれるすべての会員AIDのリンク情報を抽出する（ステップS5325）。

【0532】

6. この抽出した会員AIDのリンク情報をすべて、分割後の会員AIDのリンク情報に決定する（ステップS5327）。

【0533】

Trans PATの場合、会員AIDの決定は、図98に示すように行われる。

【0534】

1. 図101のメッセージから所有者変更したいPATを抽出し、この抽出したPATからすべての会員AIDのリンク情報を抽出する（ステップS5421）。

【0535】

2. 所有者AIDを変更後PATの会員AIDにするかチェック（ステップS5412）、会員AIDにする場合には、ステップS5421のPATから所有者AIDのリンク情報も抽出する（ステップS5423）。

【0536】

3. 残りのすべてのAIDのリンク情報をすべて、変更後PATの会員AIDのリンク情報に決定する(ステップS5425)。

【0537】

次に、AIDリストの生成について説明する。AIDリストの生成は、MakePAT、MergePAT、SplitPAT、TransPATで共通であり、図90に示すように行われる。

【0538】

1. 会員AID数をもとに、AIDリストのバッファ長を決定する(ステップS4611)。
2. この決定した情報をもとに、バッファを生成する(ステップS4612)。

【0539】

3. 所有者AIDのリンク情報をステップS4612のバッファの空き領域にコピーする(ステップS4617)。
4. 会員AIDのリンク情報をステップS4617の残りの空き領域にコピーする(ステップS4618)。

【0540】

5. 次の会員AIDが存在する場合には、ステップS4618に戻り、繰り返す(ステップS4615)。

【0541】

本実施形態の、Enablerの正当性の検証は図55を参照した前述した説明と同じである。また、このEnablerの正当性の検証は、MakePAT、MergePAT、SplitPAT、TransPATで共通である。

【0542】

【発明の効果】

以上説明したように、本発明によれば、付与情報をユーザに付与し、付与情報とユーザに関する情報とを対にして他のユーザから閲覧可能に保持し、ユーザ間の対応を示す発信者の指定情報を指定し、アクセス権を示す個別化アクセスチケットを発行し、発信者からの発信要求に対して個別化アクセスチケットを用いて

アクセス権を検証し、検証結果が正しい場合にユーザ間の接続制御を行うので、ユーザの本当の識別子を隠蔽しつつ、ユーザの特性を表す情報を公開し、この情報に基づいて適切な通信を行うことができ、従来のような第三者からの攻撃等を的確に防止することができる。加えて、着信者が匿名性を悪用した発信者による攻撃を受けた場合には、その攻撃による着信者への被害を最小限に食い止めることができる。

【0543】

また、本発明によれば、第1の個別化アクセスチケットの所有者役割識別子を第1の個別化アクセスチケット変更権(Enabler)で照合し、正しい場合に、第2の個別化アクセスチケット変更権(Enabler)、役割識別子により新たな所有者役割識別子の変更、新たな会員役割識別子の追加または会員役割識別子の削除を行い、第2の個別化アクセスチケットを作成するので、個別化アクセスチケットの新規生成、変更をユーザ主導で行うことができ、例えば動的に変化するグループ通信(メーリングリスト等)の会員の連絡先情報等も適確に管理することができる。

【0544】

更に、本発明によれば、個別化アクセスチケット(PAT)の新規生成および既存の個別化アクセスチケット(PAT)の内容変更を行うために、Null-AID(AID_{Null})および該Null-AIDのEnabler(Enabler of Null-AIDまたはEnabler of AID_{Null})を使用するので、会員AIDおよびEnabler of 会員AIDを所有者AIDに渡さなくても新規生成(MakePAT)およびマージ(MergePAT)を行うことができるとともに、また会員AIDを用いた成りすましを防止することができる。

【0545】

本発明によれば、Null-AIDは個別化アクセスチケット(PAT)の所有者AIDとしてのみ使用可能であり、

【数47】

$$PAT < AID_{Null} | AID_{\text{会員1}}, AID_{\text{会員2}}, \dots, AID_{\text{会員N}} >$$
は許可し、また

【数 48】

$$PAT < AID_{所有者} | AID_{Null}, AID_{会員1}, AID_{会員2}, \dots, AID_{会員N} >$$

は許可しないので、 $PAT < AID_{所有者} | AID_{会員} >$ の所有者が $AID_{会員}$ の Enabler を知らない場合には、この PAT から $PAT < AID_{Null} | AID_{会員} >$ を作成することはできない。

【0546】

また、本発明によれば、 $God-AID (AID_{God})$ を用いて、個別化アクセスチケット (PAT) に読取専用属性を設定するので、グループ通信において参加者を固定することができる。

【0547】

更に、本発明によれば、役割識別子は該役割識別子を一意に特定するためのリンク情報を有し、該リンク情報を個別化アクセスチケットに設定し、該個別化アクセスチケットで使用される役割識別子を前記リンク情報で特定するので、個別化アクセスチケットは役割識別子の実体を含まないため、役割識別子の実体を使用することなく着信拒否機能を実現することができる。

【図面の簡単な説明】

【図 1】

本発明において使用される役割識別子 AID 、個別化アクセスチケット PAT を示す説明図である。

【図 2】

本発明の一実施形態の全体構成図である。

【図 3】

個人識別子 OID と役割識別子 AID の例を示している。

【図 4】

ユーザが役割識別子 AID を認証局 CA に対して請求する処理を示すフローチャートである。

【図 5】

役割識別子 AID の請求に対する認証局 CA が役割識別子 AID をユーザに対

して交付する処理を示すフローチャートである。

【図6】

ユーザにおけるAID交付処理を示すフローチャートである。

【図7】

役割識別子AIDの請求メッセージの例を示す図である。

【図8】

役割識別子AIDの交付メッセージの例を示す図である。

【図9】

認証局CAにおける役割識別子AIDの生成処理を示すフローチャートである。

【図10】

図9のAID生成処理に関連する説明図である。

【図11】

アノニマス・ディレクトリ・サービスADSにおける役割識別子AIDの登録と個別化アクセスチケットPATの交付の例を示す説明図である。

【図12】

ADSにおいて個別化アクセスチケットPATを生成する場合の処理を示すフローチャートである。

【図13】

図12のPAT生成処理に関連する説明図である。

【図14】

SCSにおけるメール転送制御を示すフローチャートである。

【図15】

SCSにおける移転制御を示すフローチャートである。

【図16】

ユーザにおける移転制御を示すフローチャートである。

【図17】

SCSにおける移転制御を示すフローチャートである。

【図18】

SCSにおける個別化アクセスチケットPATに対する接続制御を示すフローチャートである。

【図19】

SCSにおけるメール返信処理を示すフローチャートである。

【図20】

ユーザ間の電子メールの例を示す図である。

【図21】

着信拒否された場合の電子メールの例を示す図である。

【図22】

ユーザにおける着信拒否申請処理を示すフローチャートである。

【図23】

SCSにおける着信拒否設定処理を示すフローチャートである。

【図24】

着信拒否申請メッセージおよび着信拒否通知メッセージの例を示す図である。

【図25】

役割識別子AIDについて個人識別子OIDの同一性を判定する処理を示すフローチャートである。

【図26】

図25に示す同一性判定処理に関連する役割識別子AIDおよび個人識別子OIDの例を示す図である。

【図27】

アナログ公衆網における二重番号登録を示す説明図である。

【図28】

アナログ公衆網における発信者番号通知を示す説明図である。

【図29】

デジタル携帯網およびアナログ公衆網における着信拒否を示す説明図である。

【図30】

匿名電子メールの説明図である。

【図 3 1】

本発明の第 2 の実施形態に使用される O I D, A I D, P A T のデータ構造を示す図である。

【図 3 2】

本発明の第 2 の実施形態に使用される Enabler のデータ構造を示す図である。

【図 3 3】

本発明の第 2 の実施形態に使用される演算規則 (Make P A T) の定義を示す図である。

【図 3 4】

本発明の第 2 の実施形態に使用される演算規則 (Merge P A T) の定義を示す図である。

【図 3 5】

本発明の第 2 の実施形態に使用される演算規則 (Split P A T) の定義を示す図である。

【図 3 6】

本発明の第 2 の実施形態に使用される演算規則 (Trans P A T) の定義を示す図である。

【図 3 7】

本発明の第 2 の実施形態に使用される装置構成 (1) を示す図である。

【図 3 8】

本発明の第 2 の実施形態に使用される装置構成 (2) を示す図である。

【図 3 9】

本発明の第 2 の実施形態に使用される装置構成 (3) を示す図である。

【図 4 0】

本発明の第 2 の実施形態に使用される装置構成 (4) を示す図である。

【図 4 1】

本発明の第 2 の実施形態に使用される装置構成 (5) を示す図である。

【図 4 2】

本発明の第 2 の実施形態に使用される装置構成 (6) を示す図である。

【図 4 3】

本発明の第 2 の実施形態に使用される装置構成 (7) を示す図である。

【図 4 4】

本発明の第 2 の実施形態の処理全体の流れ (MakePAT, MergePAT, TransPAT) を示すフローチャートである。

【図 4 5】

本発明の第 2 の実施形態の処理全体の流れ (SplitPAT) を示すフローチャートである。

【図 4 6】

本発明の第 2 の実施形態における AID リストの生成処理 (MakePAT, MergePAT, SplitPAT, TransPAT) を示すフローチャートである。

【図 4 7】

本発明の第 2 の実施形態における所有者 AID の決定処理 (MakePAT) を示すフローチャートである。

【図 4 8】

本発明の第 2 の実施形態における所有者 AID の決定処理 (MergePAT) を示すフローチャートである。

【図 4 9】

本発明の第 2 の実施形態における所有者 AID の決定処理 (SplitPAT) を示すフローチャートである。

【図 5 0】

本発明の第 2 の実施形態における所有者 AID の決定処理 (TransPAT) を示すフローチャートである。

【図 5 1】

本発明の第 2 の実施形態における会員 AID の決定処理 (MakePAT) を示すフローチャートである。

【図 5 2】

本発明の第 2 の実施形態における会員 AID の決定処理 (MergePAT) を示すフローチャートである。

【図 53】

本発明の第2の実施形態における会員AIDの決定処理 (Split PAT) を示すフローチャートである。

【図 54】

本発明の第2の実施形態における会員AIDの決定処理 (Trans PAT) を示すフローチャートである。

【図 55】

本発明の第2の実施形態におけるEnabler の正当性の検証処理 (Make PAT, Merge PAT, Split PAT, Trans PAT) を示すフローチャートである。

【図 56】

本発明の第2の実施形態におけるMakePAT命令を含むメッセージを示す図である。

【図 57】

本発明の第2の実施形態におけるMerge PAT命令を含むメッセージを示す図である。

【図 58】

本発明の第2の実施形態におけるSplit PAT命令を含むメッセージを示す図である。

【図 59】

本発明の第2の実施形態におけるTrans PAT命令を含むメッセージを示す図である。

【図 60】

本発明の第2の実施形態の一元管理型メーリングリストへの適用例を示す図である。

【図 61】

本発明の第3の実施形態に使用されるNull-AIDのデータ構造を示す図である。

【図 62】

本発明の第3の実施形態に使用される Enabler of Null-AIDのデータ

構造を示す図である。

【図 63】

本発明の第3の実施形態の第1の応用例を示す図である。

【図 64】

本発明の第3の実施形態の第2の応用例を示す図である。

【図 65】

本発明の第4の実施形態に使用されるGod-AIDのデータ構造を示す図である。

【図 66】

本発明の第4の実施形態におけるGod-AID規則の処理を示すフローチャートである。

【図 67】

本発明の第4の実施形態の第1の応用例を示す図である。

【図 68】

本発明の第4の実施形態の第2の応用例を示す図である。

【図 69】

本発明の第5の実施形態における会員AIDのチェック処理を示すフローチャートである。

【図 70】

本発明の第6の実施形態の全体構成図である。

【図 71】

第6の実施形態に使用される個人識別子OID、リンク情報付き役割識別子AID、リンク指定型1対1個別化アクセスチケットPATの例を示している。

【図 72】

認証局CAにおける役割識別子AIDの生成処理を示すフローチャートである。

【図 73】

図72のAID生成処理に関連する説明図である。

【図 74】

アノニマス・ディレクトリ・サービスADSにおける役割識別子AIDの登録と個別化アクセスチケットPATの交付の例を示す説明図である。

【図 75】

ADSにおいてリンク指定型1対1個別化アクセスチケットPATを生成する場合の処理を示すフローチャートである。

【図 76】

図 75 の PAT 生成処理に関連する説明図である。

【図 77】

SCSにおけるメール転送制御を示すフローチャートである。

【図 78】

SCSにおけるリンク指定型1対1個別化アクセスチケットPATに対する経路制御を示すフローチャートである。

【図 79】

リンク情報付き役割識別子AIDについて個人識別子OIDの同一性を判定する処理を示すフローチャートである。

【図 80】

図 79 に示す同一性判定処理に関連するリンク情報付き役割識別子AIDおよび個人識別子OIDの例を示す図である。

【図 81】

本発明の第7の実施形態に使用される個人識別子OID、リンク情報付き役割識別子AID、リンク指定型1対N個別化アクセスチケットPATのデータ構造を示す図である。

【図 82】

本発明の第7の実施形態に使用されるEnabler のデータ構造を示す図である。

【図 83】

本発明の第7の実施形態に使用される装置構成(1)を示す図である。

【図 84】

本発明の第7の実施形態に使用される装置構成(2)を示す図である。

【図 85】

本発明の第7の実施形態に使用される装置構成(3)を示す図である。

【図 86】

本発明の第7の実施形態に使用される装置構成(4)を示す図である。

【図 87】

本発明の第7の実施形態に使用される装置構成(5)を示す図である。

【図 88】

本発明の第7の実施形態に使用される装置構成(6)を示す図である。

【図 89】

本発明の第7の実施形態に使用される装置構成(7)を示す図である。

【図 90】

本発明の第7の実施形態におけるAIDリストの生成処理(MakePAT, MergePAT, SplitPAT, TransPAT)を示すフローチャートである。

【図 91】

本発明の第7の実施形態における所有者AIDの決定処理(MergePAT)を示すフローチャートである。

【図 92】

本発明の第7の実施形態における所有者AIDの決定処理(MakePAT)を示すフローチャートである。

【図 93】

本発明の第7の実施形態における所有者AIDの決定処理(SplitPAT)を示すフローチャートである。

【図 94】

本発明の第7の実施形態における所有者AIDの決定処理(TransPAT)を示すフローチャートである。

【図 95】

本発明の第7の実施形態における会員AIDの決定処理(MakePAT)を示すフローチャートである。

【図96】

本発明の第7の実施形態における会員AIDの決定処理（Merge PAT）を示すフローチャートである。

【図97】

本発明の第7の実施形態における会員AIDの決定処理（Split PAT）を示すフローチャートである。

【図98】

本発明の第7の実施形態における会員AIDの決定処理（Trans PAT）を示すフローチャートである。

【図99】

本発明の第7の実施形態におけるMerge PAT命令を含むメッセージを示す図である。

【図100】

本発明の第7の実施形態におけるSplit PAT命令を含むメッセージを示す図である。

【図101】

本発明の第7の実施形態におけるTrans PAT命令を含むメッセージを示す図である。

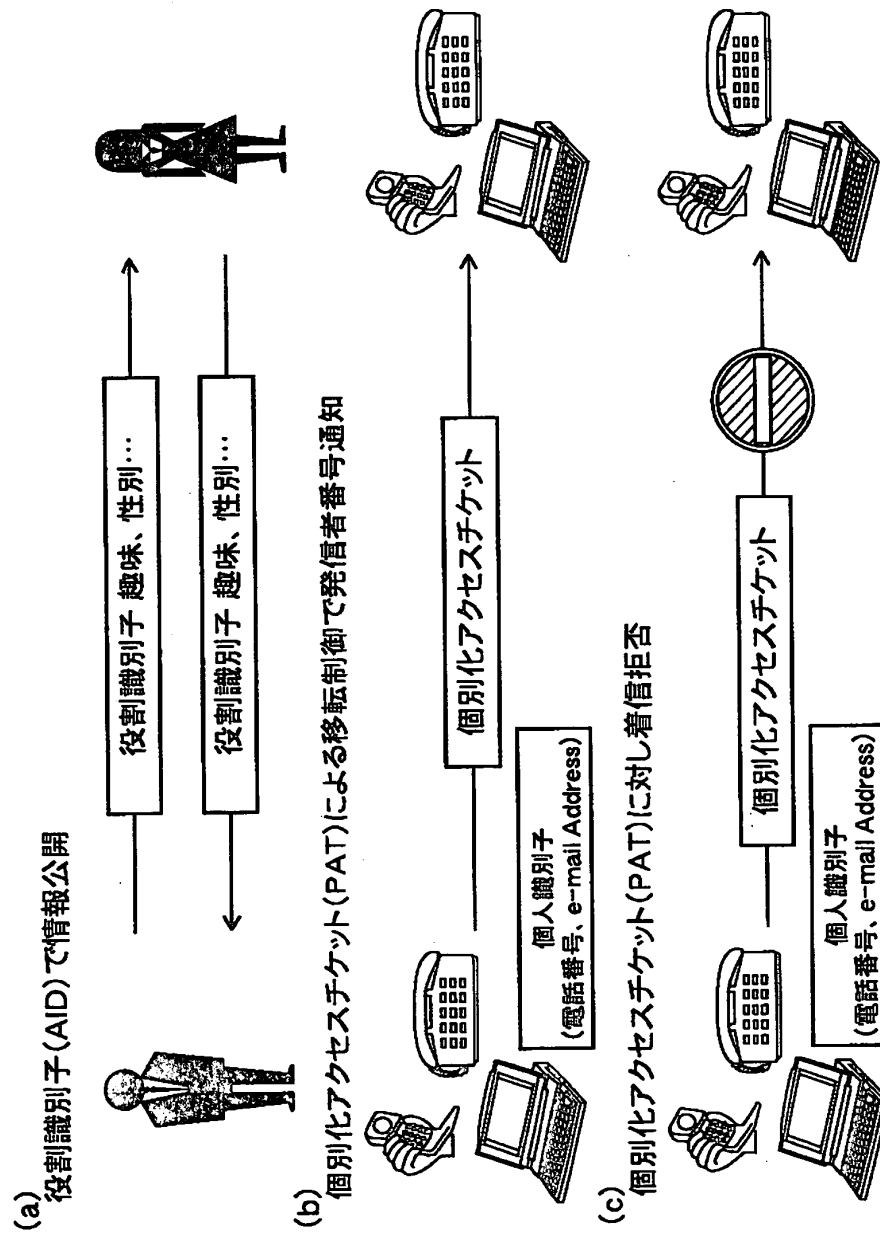
【符号の説明】

- 1 認証局CA
- 3 ユーザ
- 5 セキュア・コミュニケーション・サービスSCS
- 7 アノニマス・ディレクトリ・サービスADS

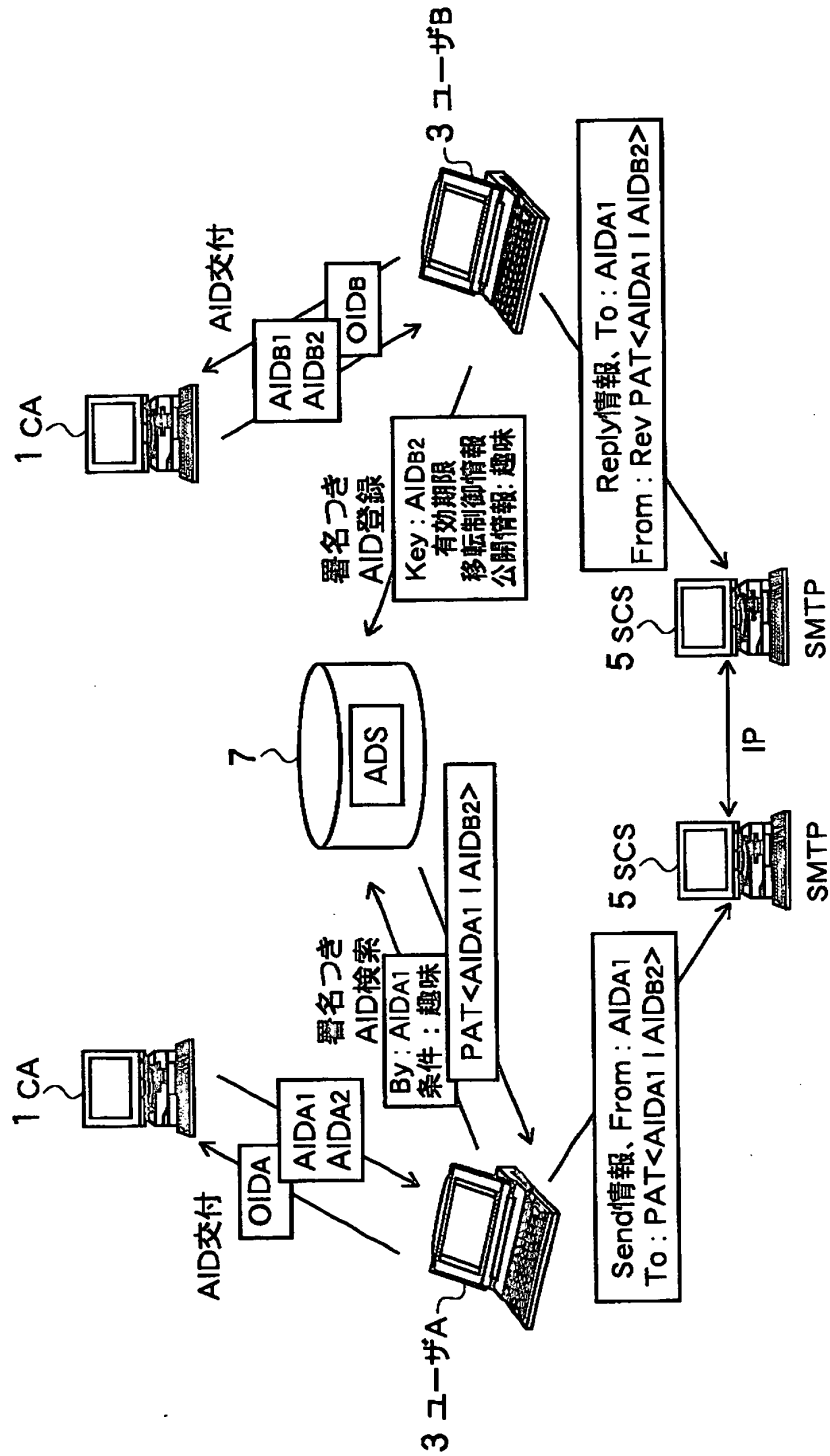
【書類名】

図面

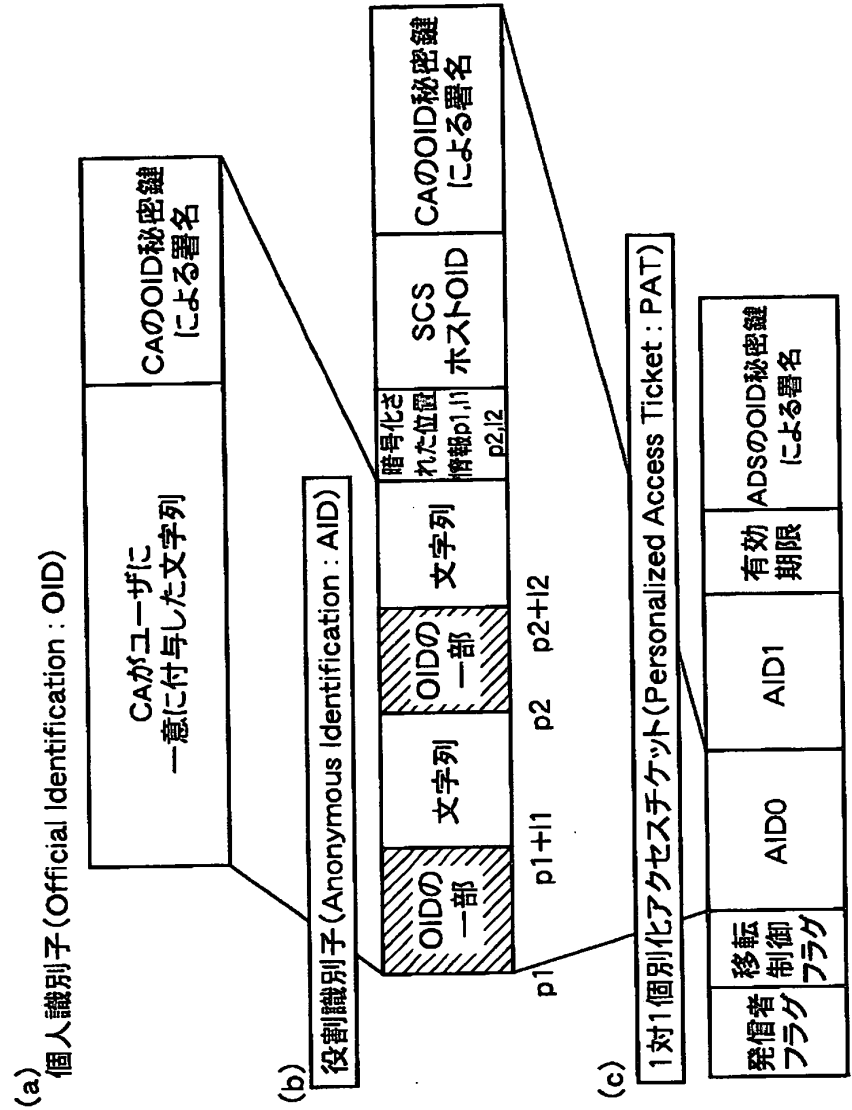
【図 1】



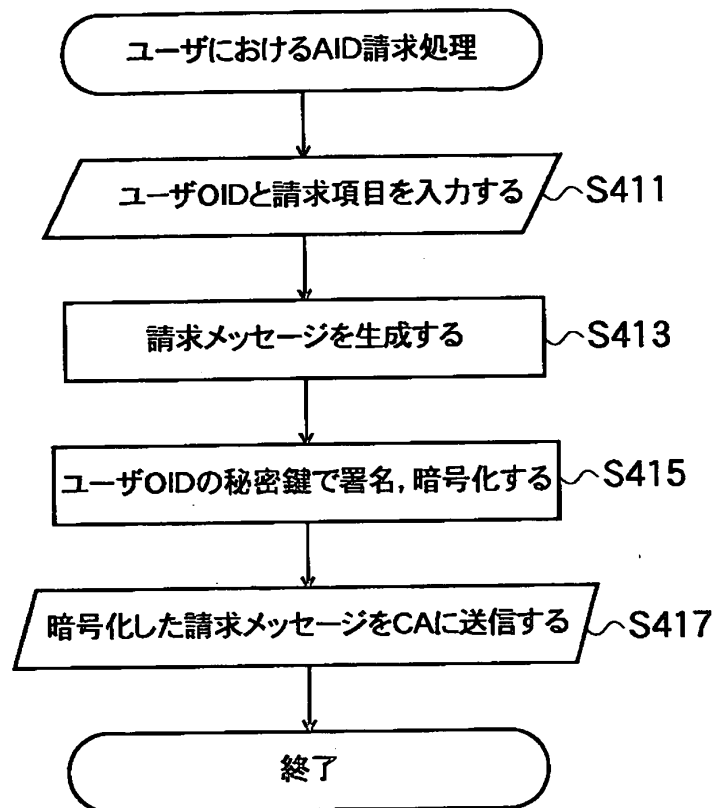
【図2】



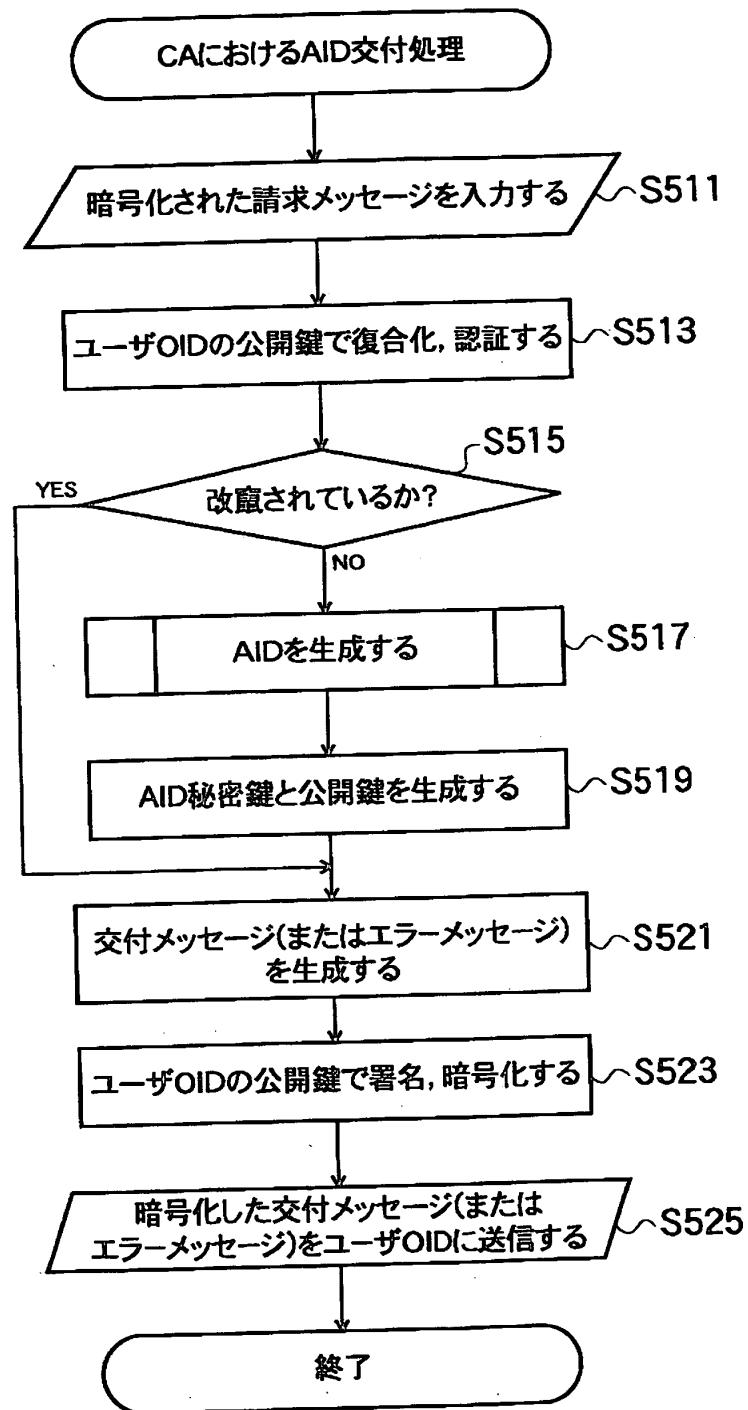
【図3】



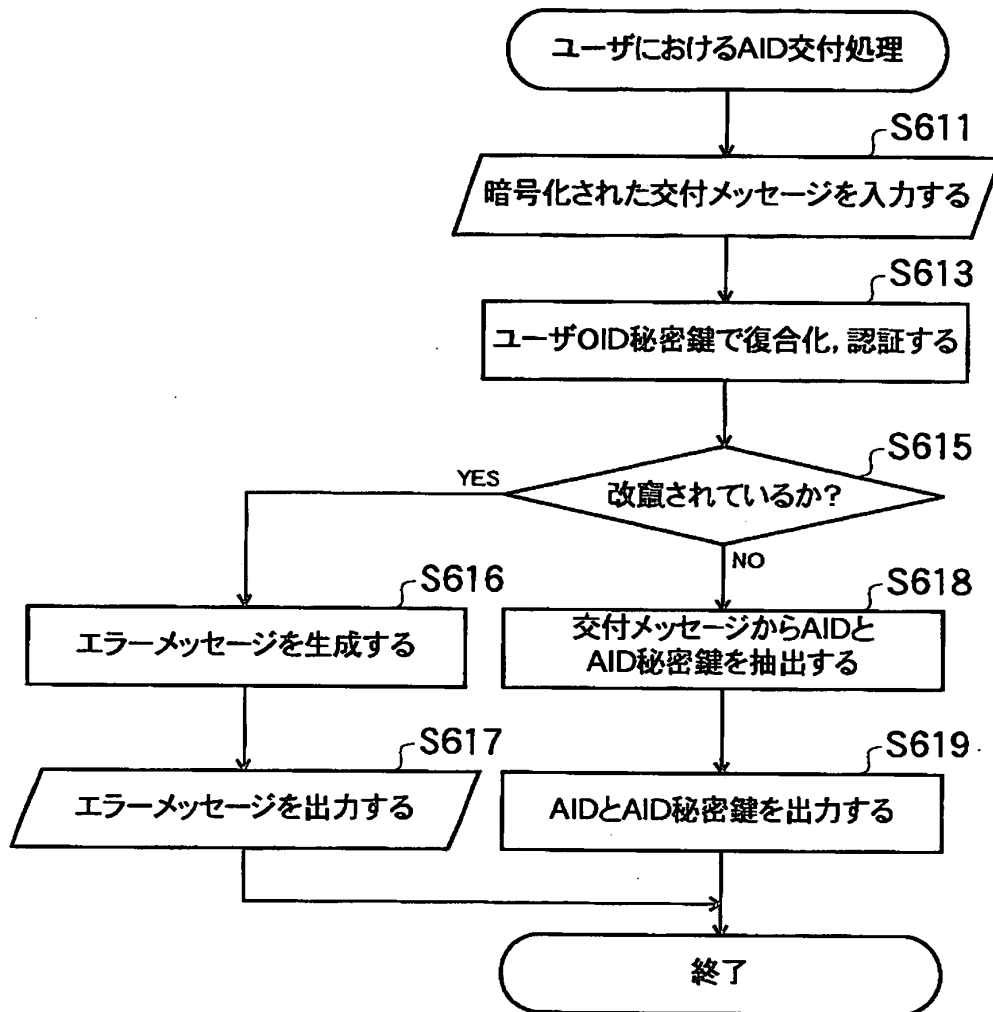
【図4】



【図5】



【図6】



【図7】

AID請求メッセージの例

REQUEST AID 2 (新規AIDを2個請求する場合)

<ユーザOIDの秘密鍵による署名>
(送信時には、ユーザOIDの秘密鍵で暗号化する)

DISCARD AID AID1の実体 AID1の秘密鍵
DISCARD AID AID2の実体 AID2の秘密鍵
(既存AIDであるAID1とAID2を廃止したい場合)

<ユーザOID秘密鍵による署名>
(送信時には、ユーザOIDの秘密鍵で暗号化する)

【図8】

AID交付メッセージの例

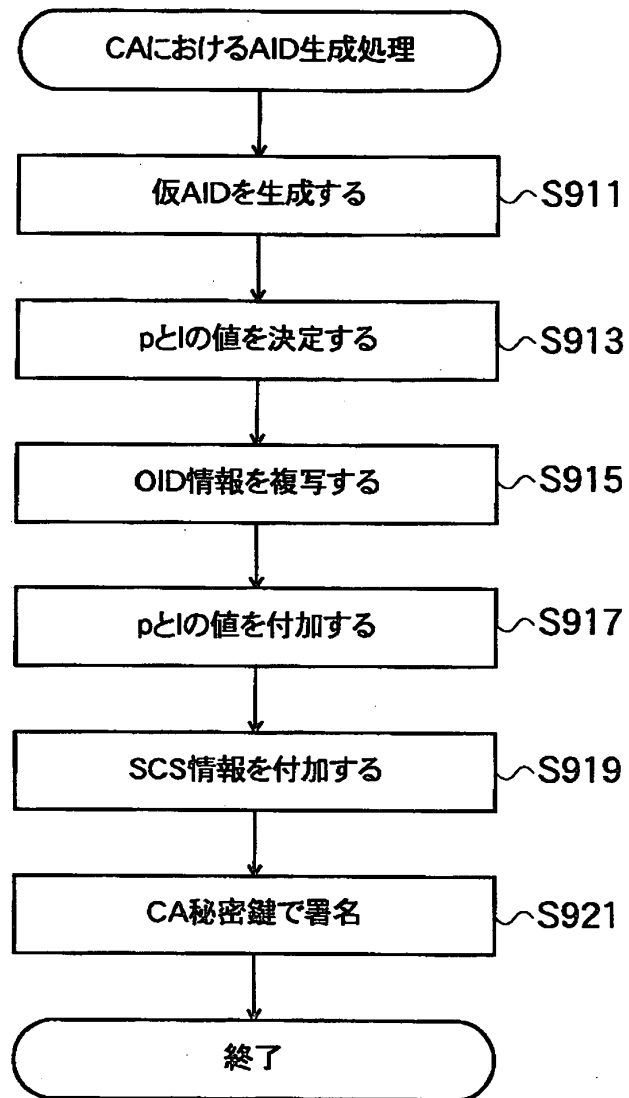
NEW AID AID3の実体 AID3の秘密鍵 OK
(新規AIDであるAID3は交付成功)
NEW AID NG (交付失敗,つまり,エラーメッセージ)

<ユーザOIDの公開鍵による署名>
(送信時には、ユーザOIDの公開鍵で暗号化する)

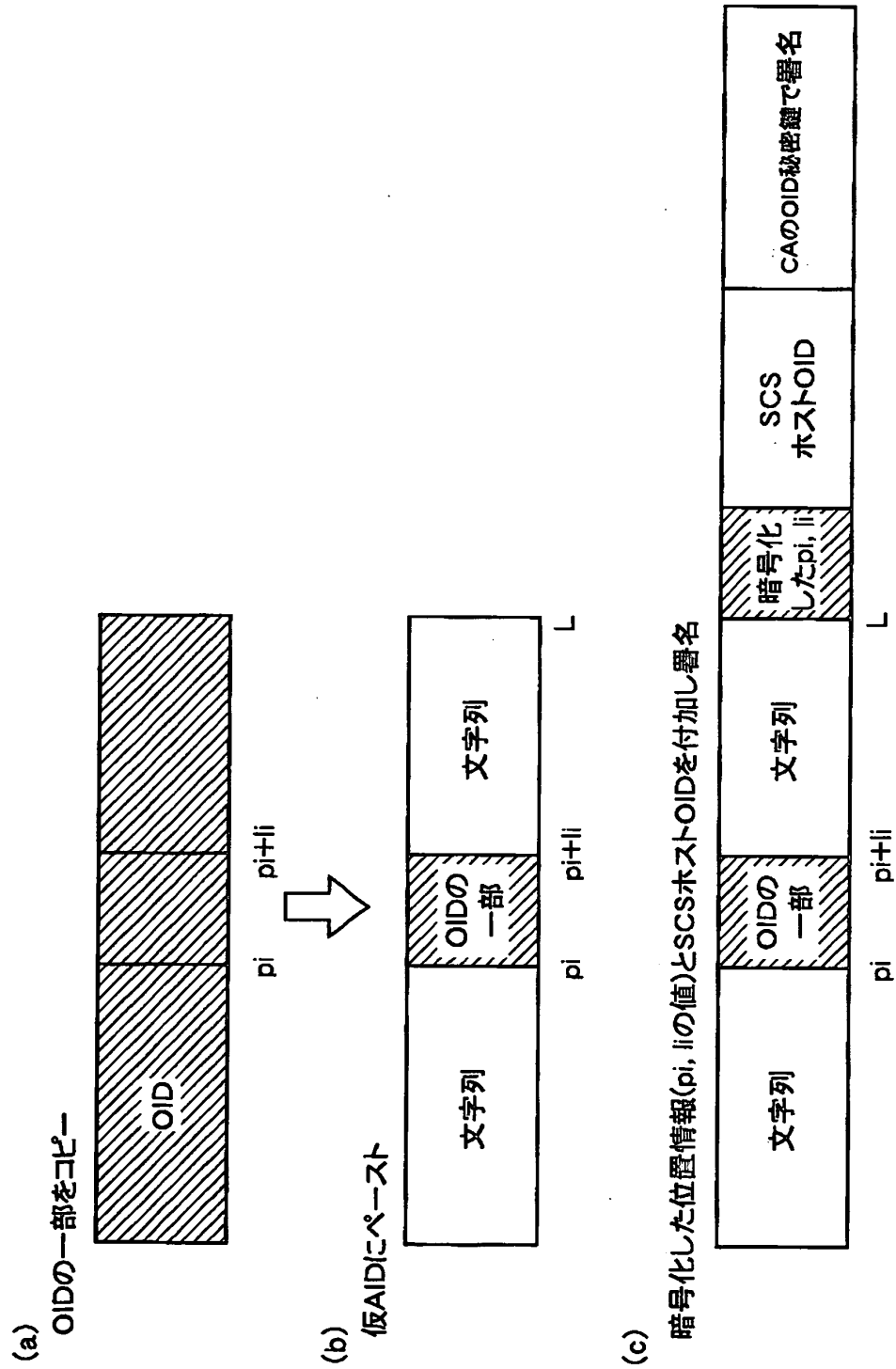
DISCARD AID AID1の実体 OK (既存AIDであるAID1は廃止成功)
DISCARD AID AID2の実体 NG
(既存AIDであるAID2の廃止失敗のエラーメッセージ)

<ユーザOIDの公開鍵による署名>
(送信時には、ユーザOIDの公開鍵で暗号化する)

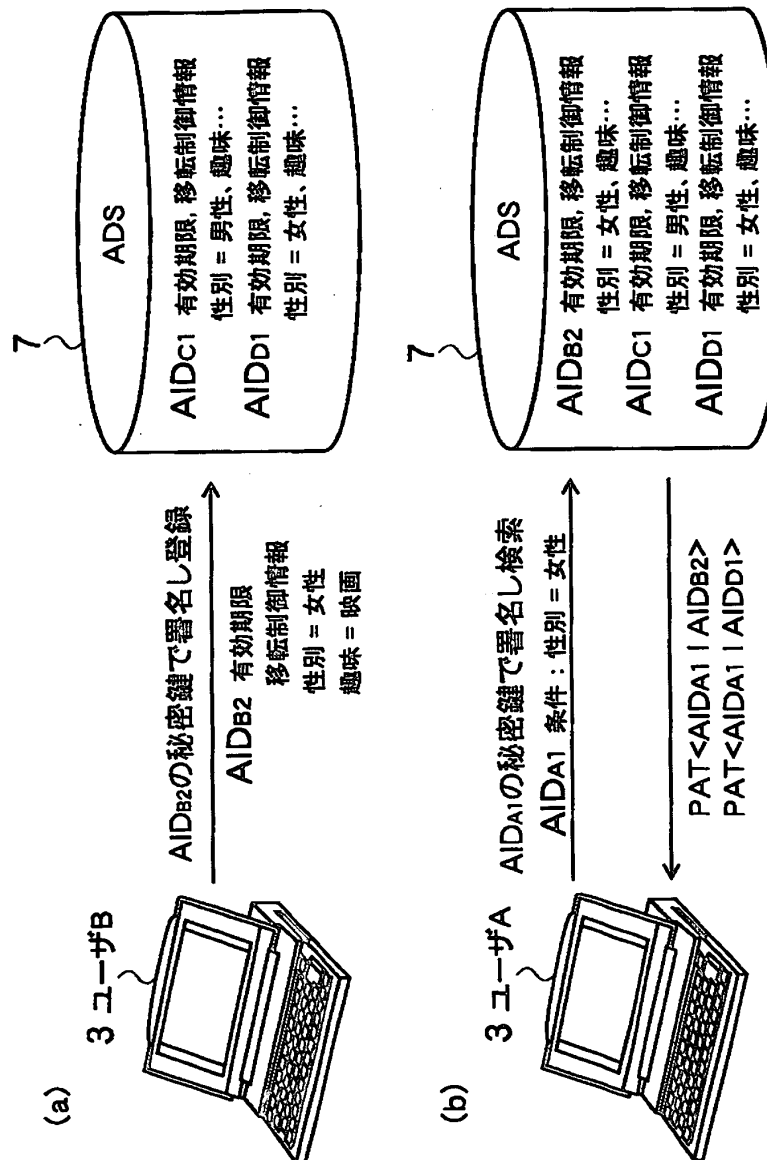
【図9】



【図 10】

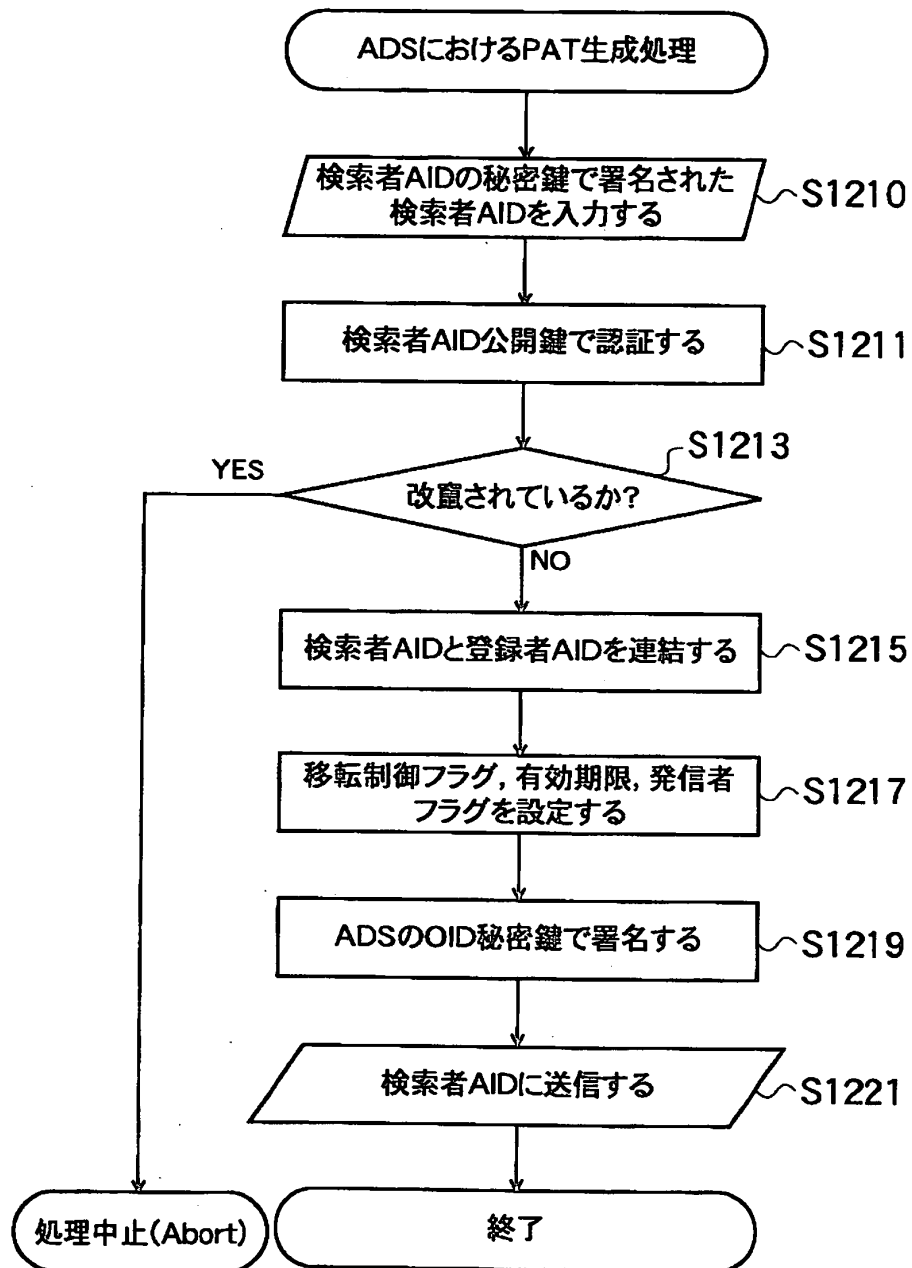


【図11】

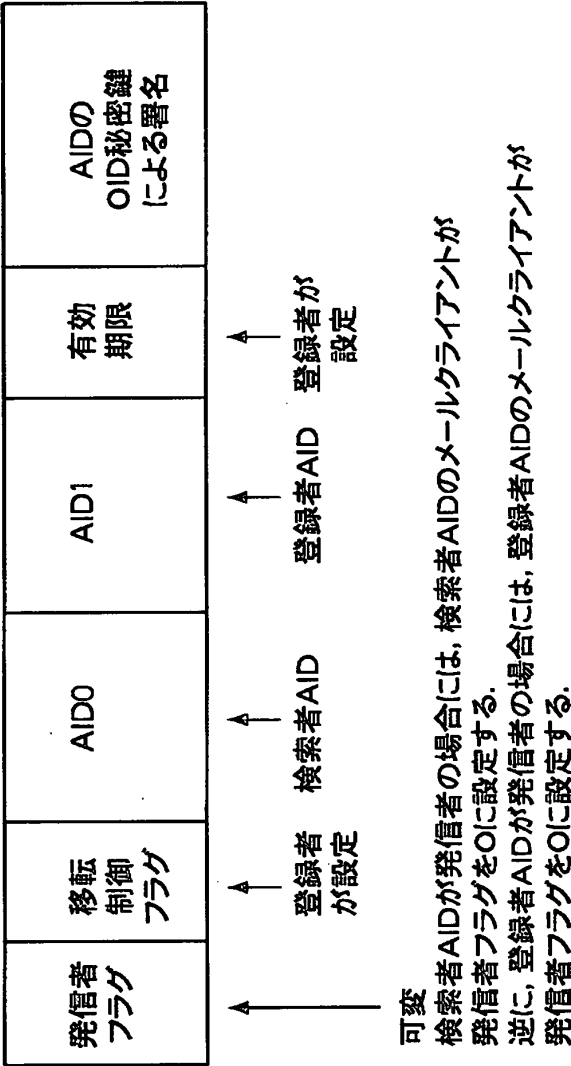


ADSにおけるAID登録とPAT交付の例

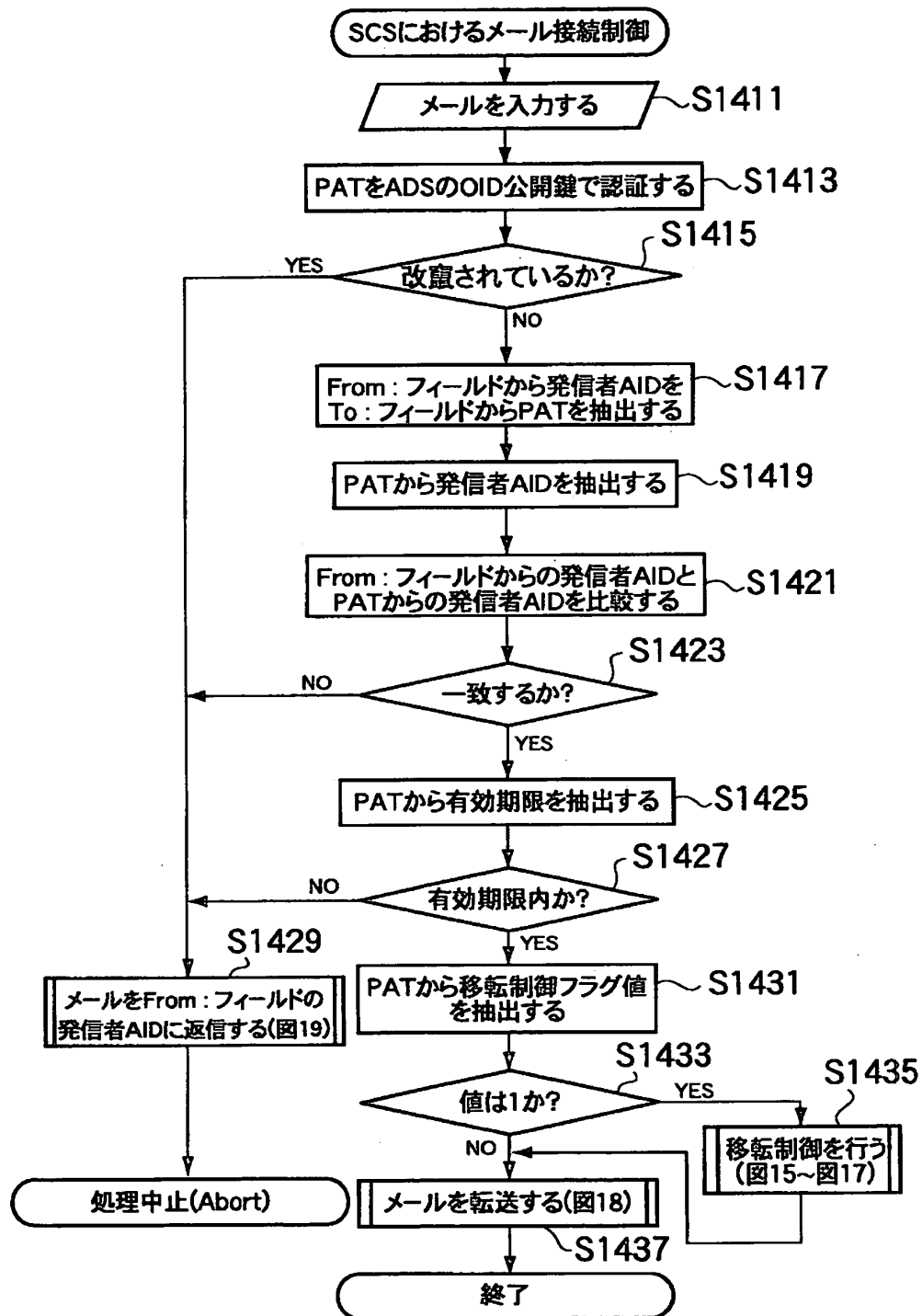
【図 12】



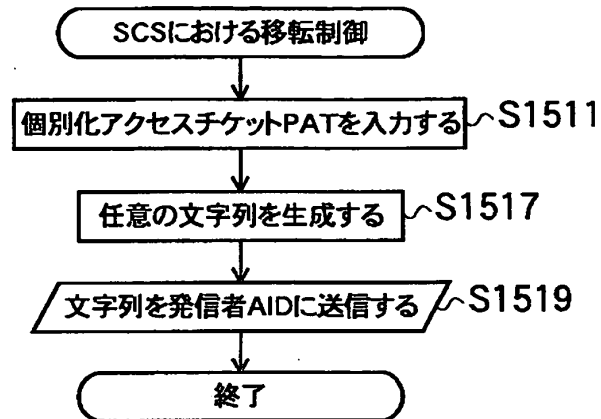
【図13】



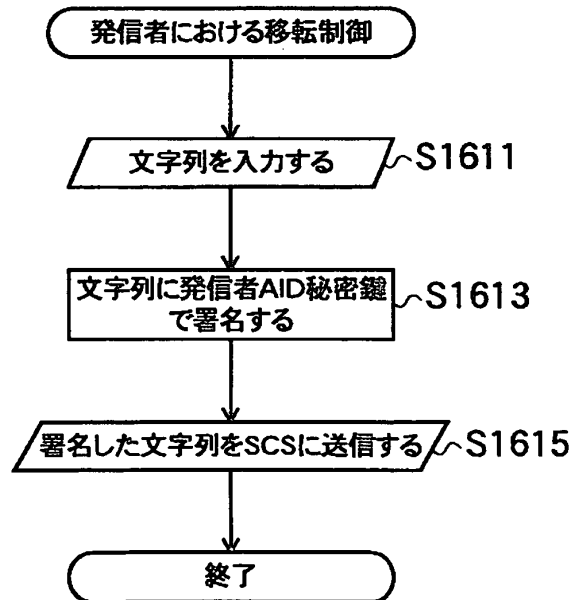
【図 14】



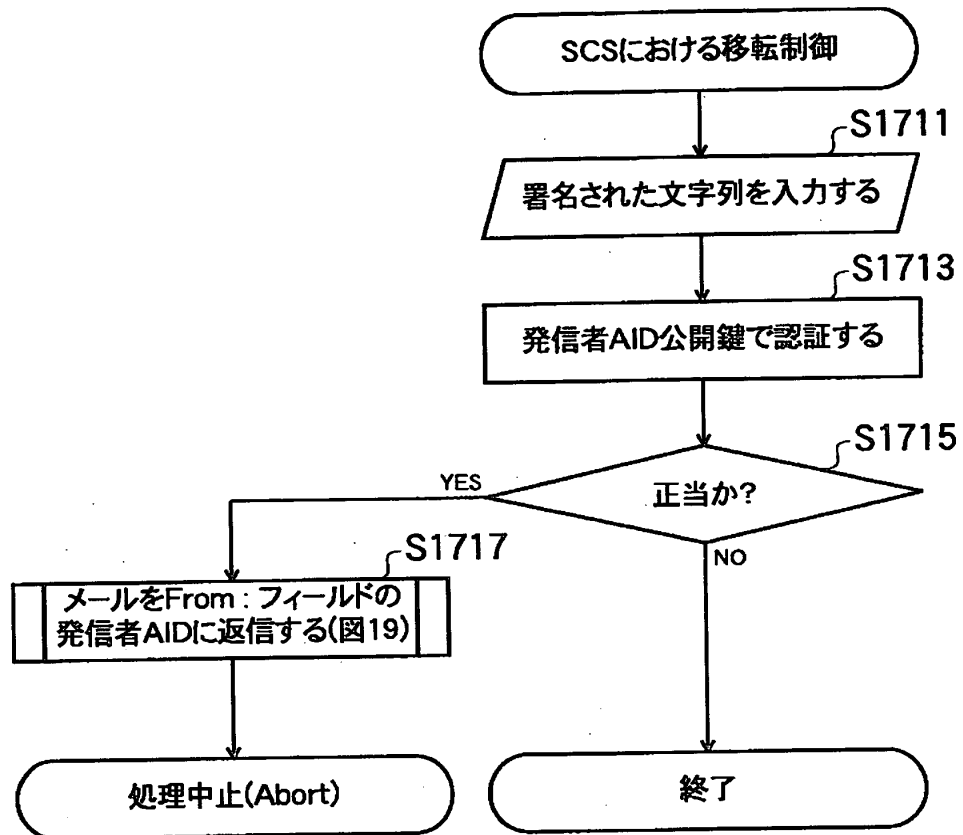
【図 15】



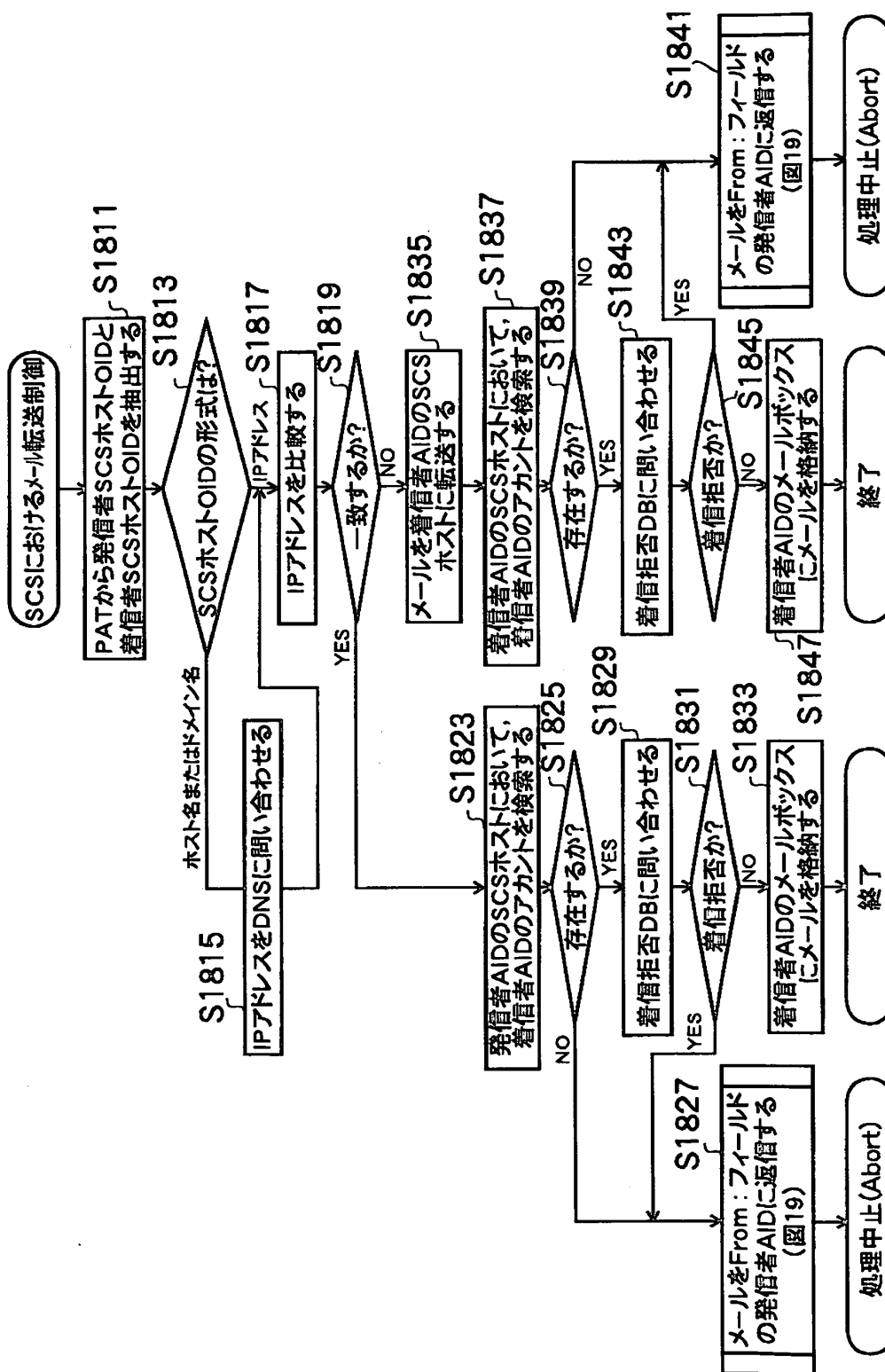
【図 16】



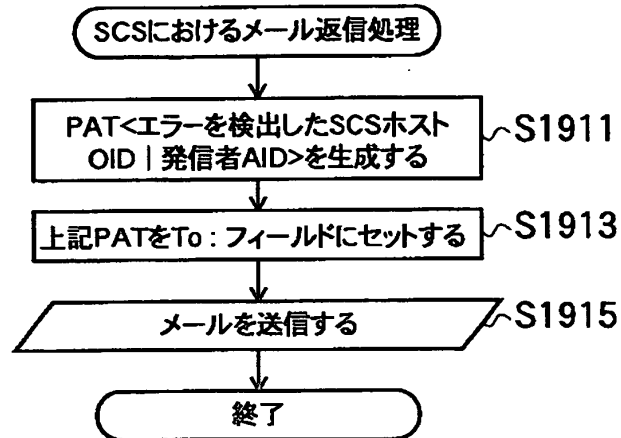
【図 17】



【图 18】



【図 19】



【図 20】

クライアント間の電子メールの例

送信

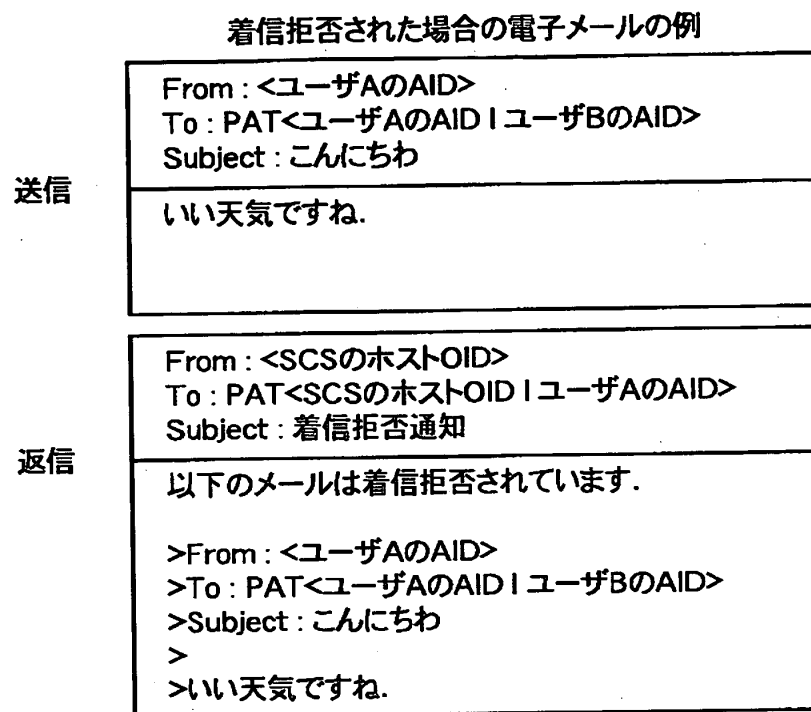
From : <ユーザAのAID> To : PAT<ユーザAのAID ユーザBのAID> Subject : こんにちは
いい天気ですね.

返信

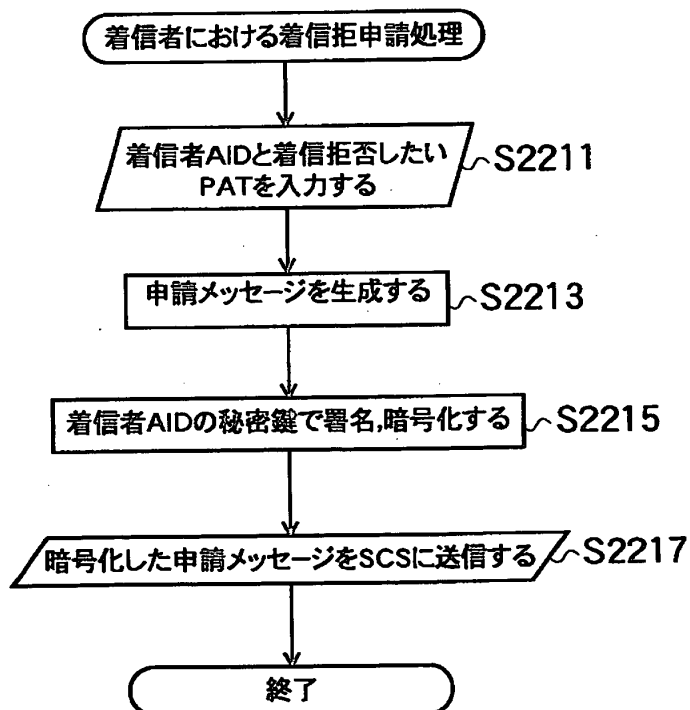
From : <ユーザBのAID> To : Rev PAT<ユーザAのAID ユーザBのAID> Subject : Re : こんにちは
そうですね.

PAT<A | B>は発信者フラグが0(つまり発信者はA)のPAT
Rev PAT<A | B>は発信者フラグが1(つまり発信者はB)のPAT

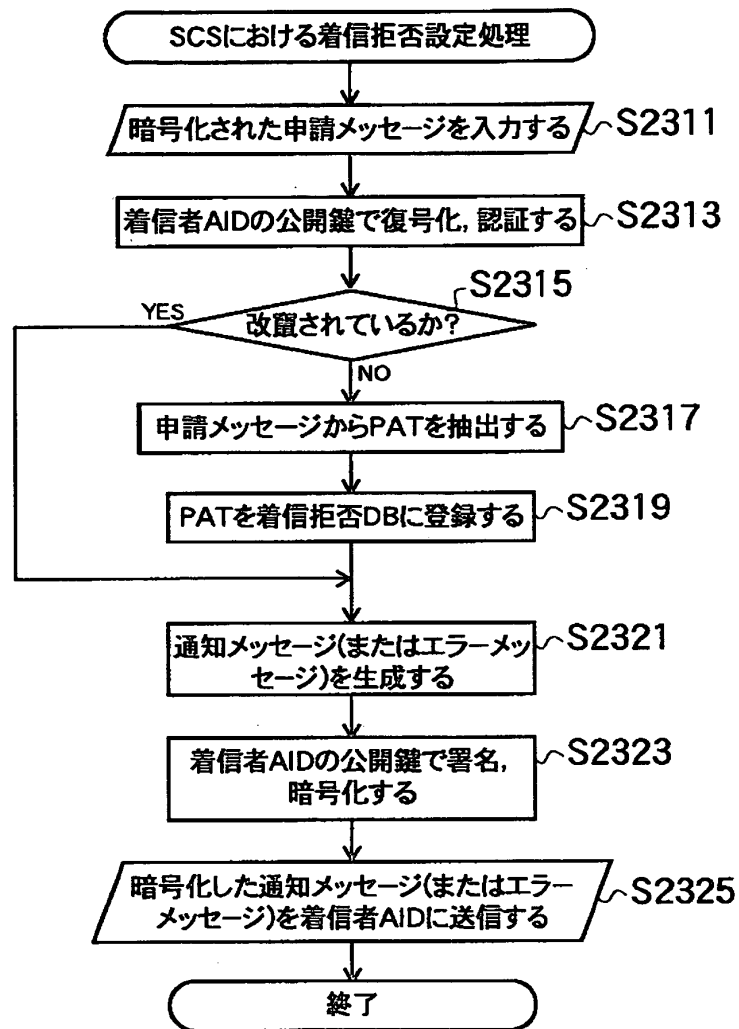
【図 21】



【図 22】



【図 23】



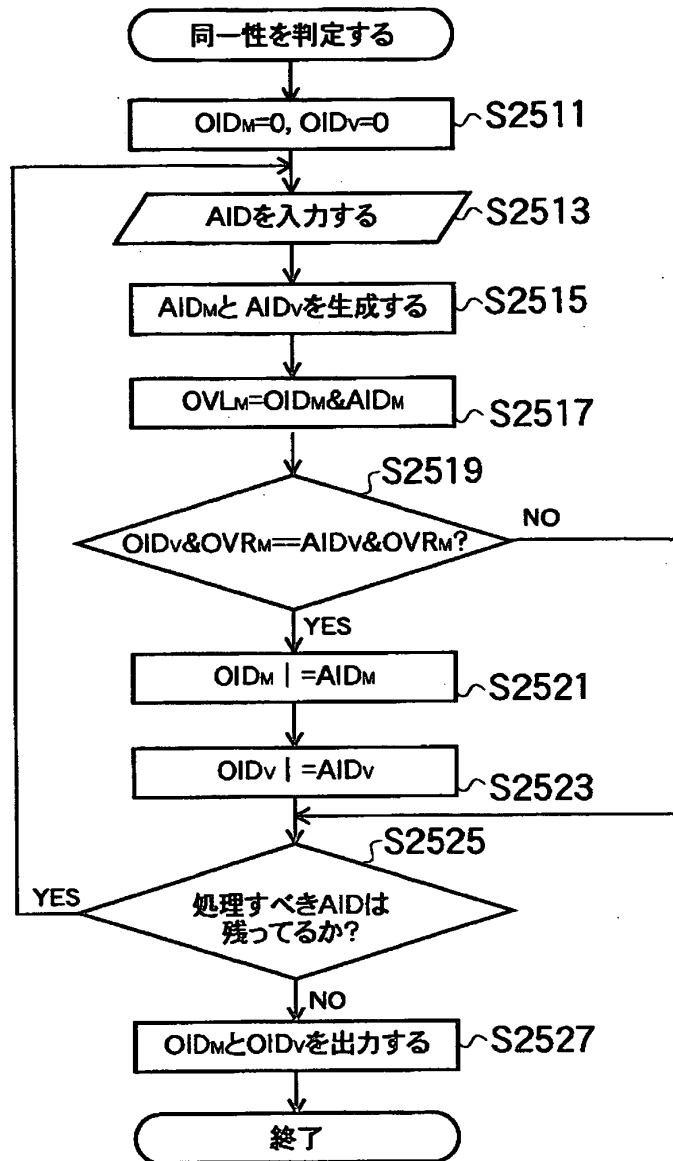
【図 24】

着信拒否申請・通知メッセージの例

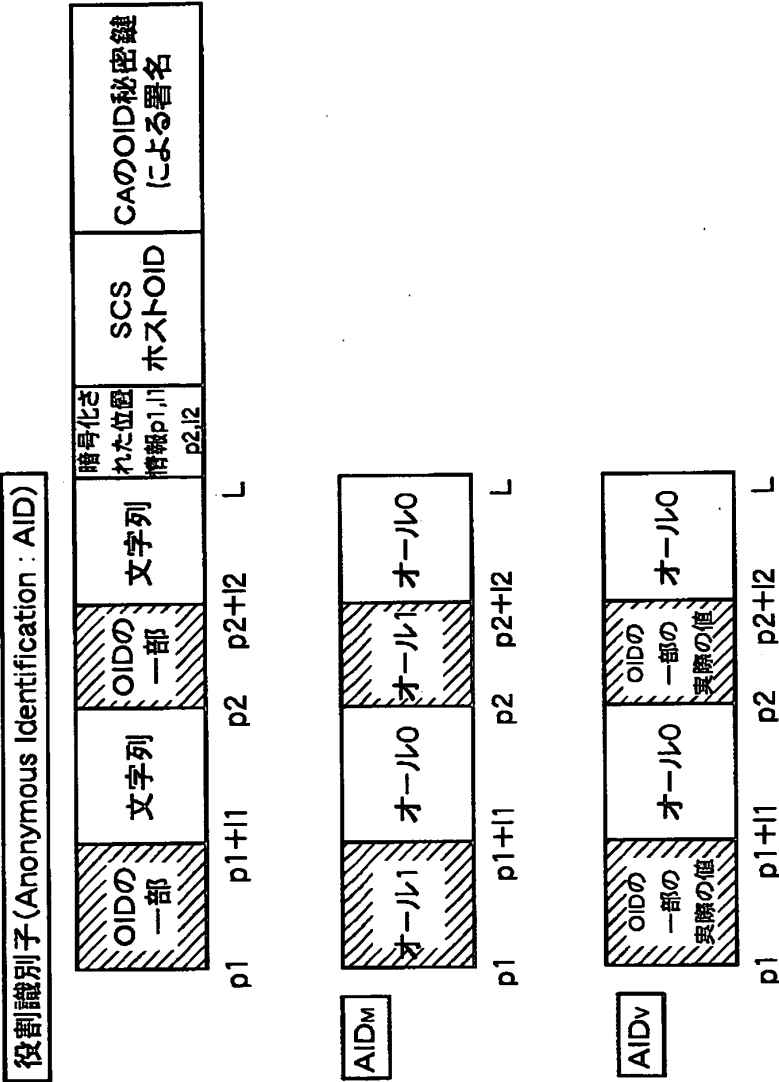
AIDの実体 REFUSE	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の設定の場合)
AIDの実体 RECONNECT	PAT, IPアドレス, ホスト名, ドメイン名の実体 (着信拒否の解除の場合)
<着信者AIDの秘密鍵による署名>	

AIDの実体 REFUSE	OKPAT, IPアドレス, ホスト名, ドメイン名の実体 (設定成功の場合)
AIDの実体 RECONNECT	NGPAT, IPアドレス, ホスト名, ドメイン名の実体 (解除失敗の場合, つまり, エラーメッセージ)
<着信者AIDの公開鍵による署名>	

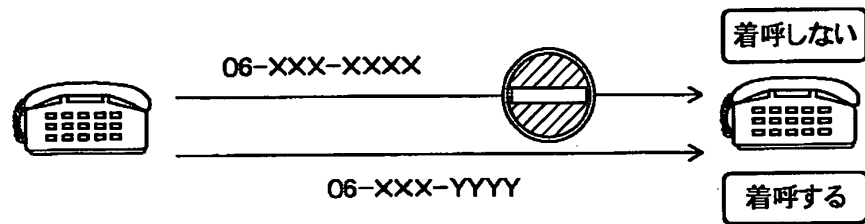
【図25】



【図26】

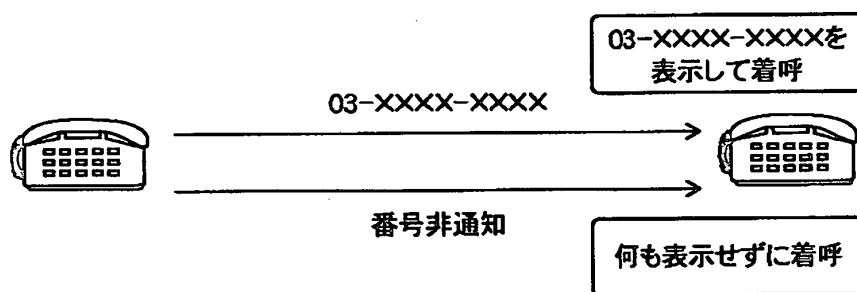


【図27】



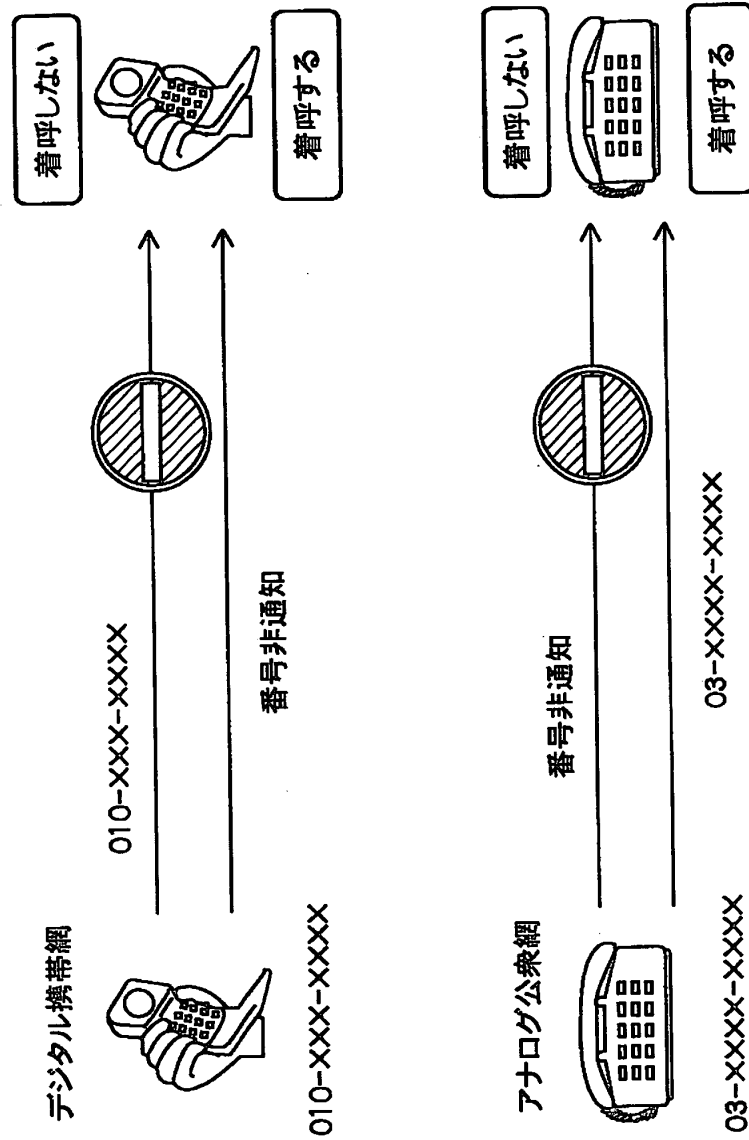
アナログ公衆網における二重番号登録

【図28】



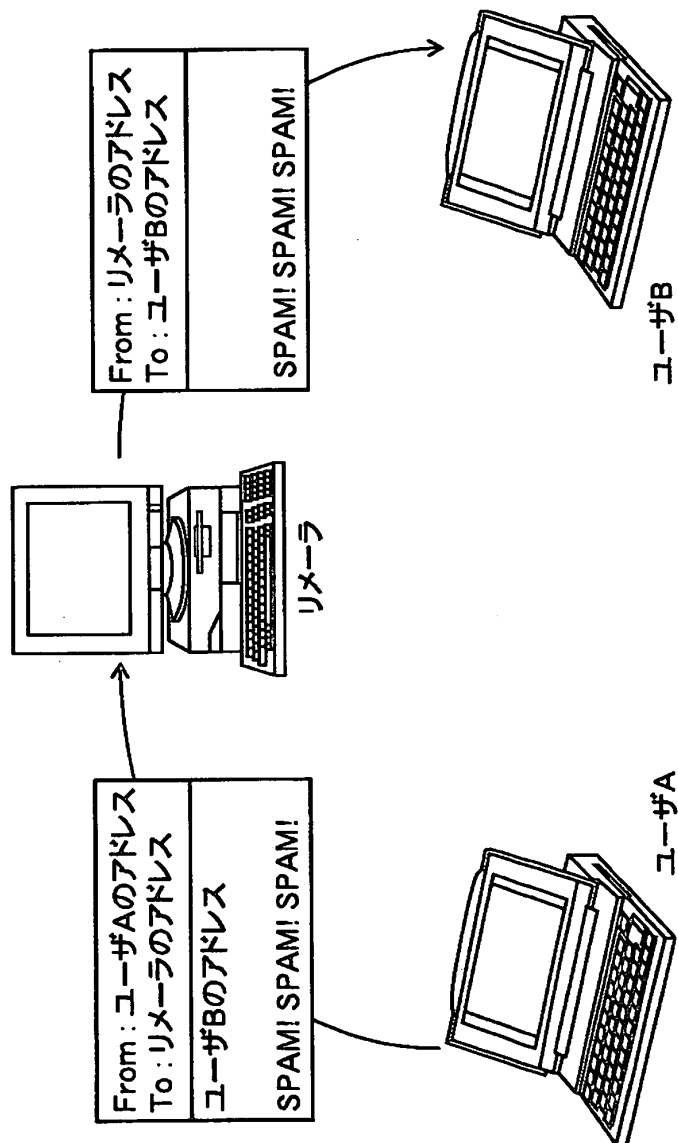
アナログ公衆網における発信者番号通知

【図29】



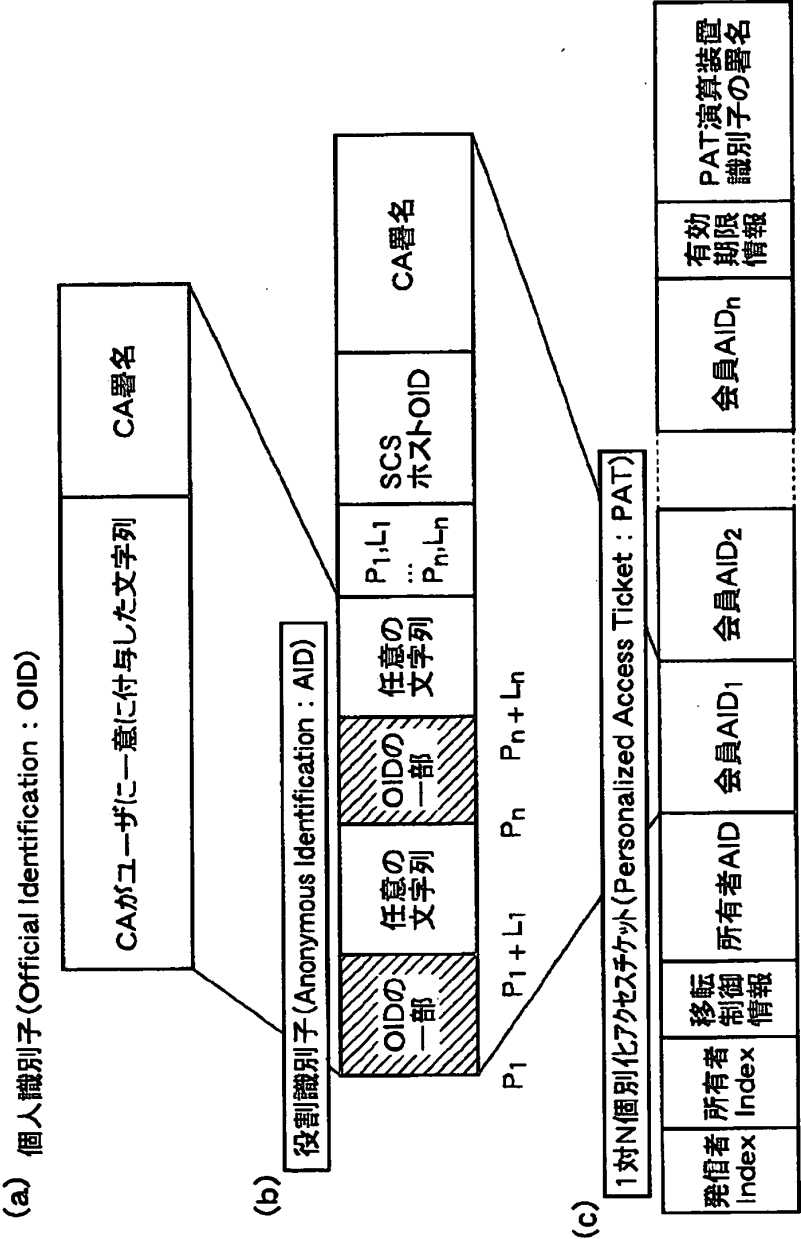
デジタル携帯網・アナログ公衆網における着信拒否

【図 30】

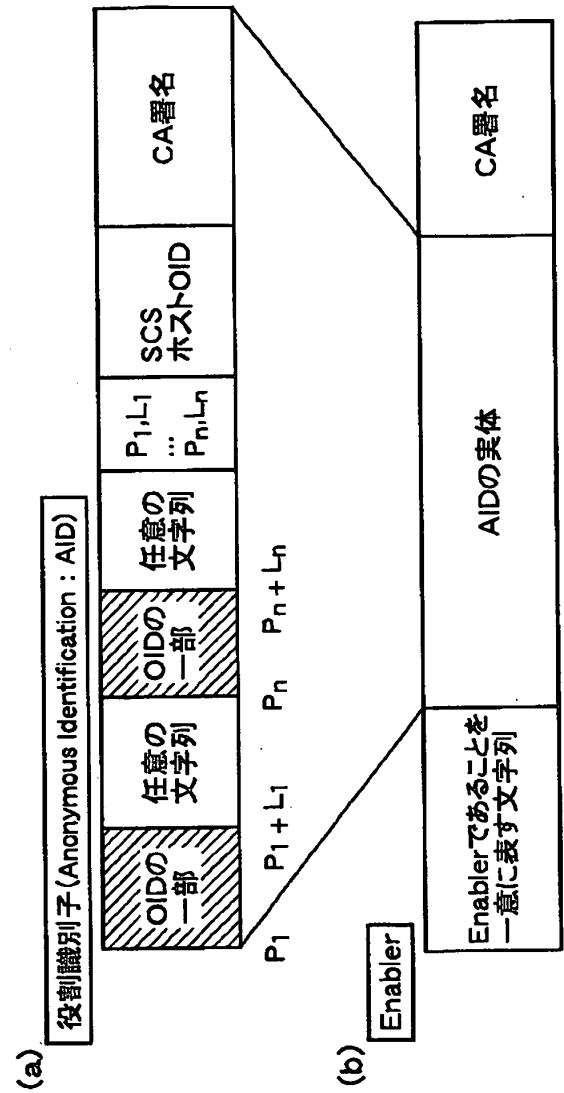


匿名電子メール (Anonymous Mails)

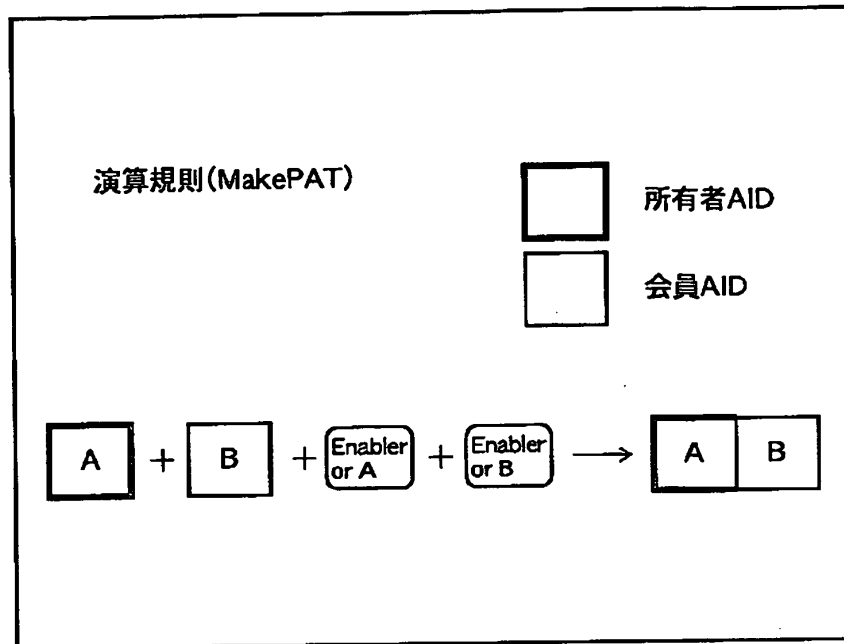
【図31】



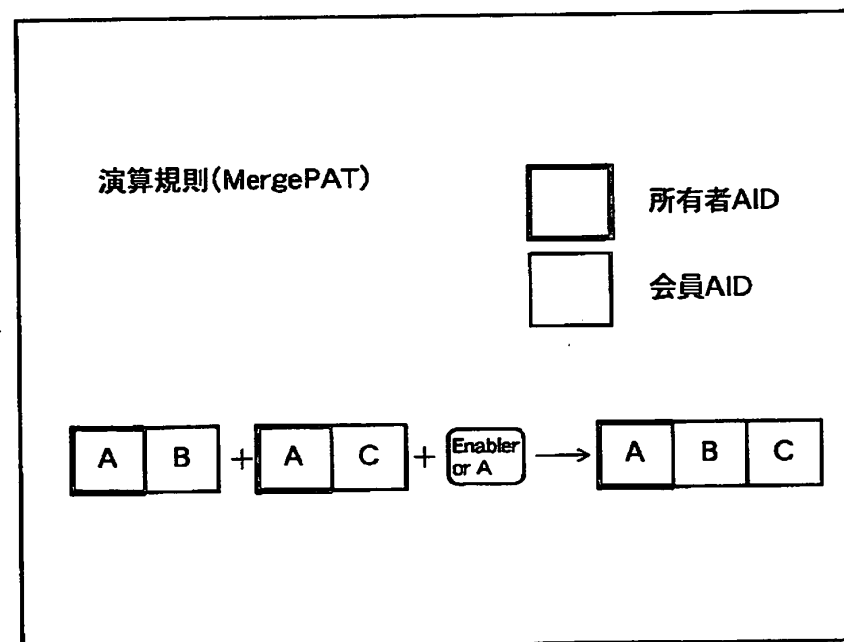
【図32】



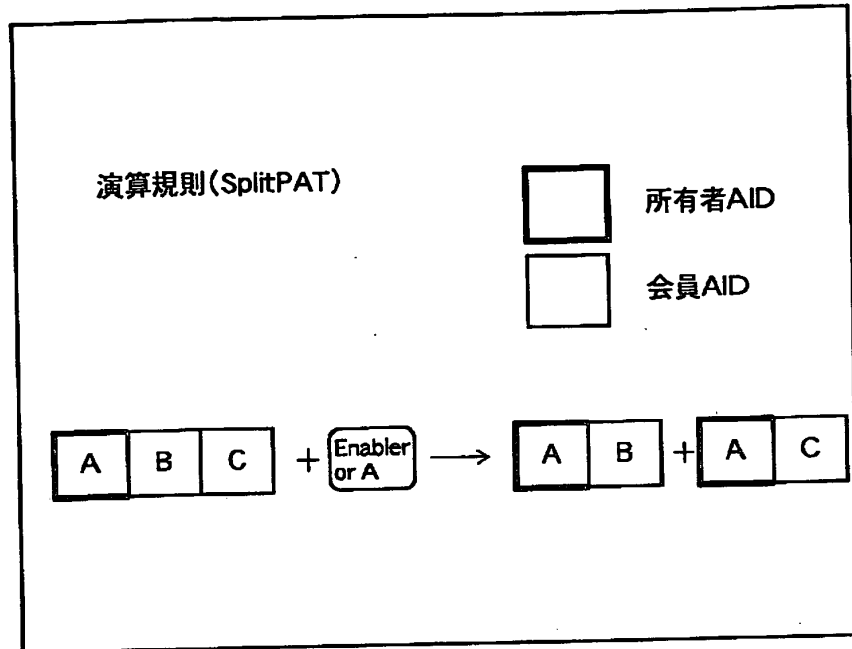
【図 3 3】



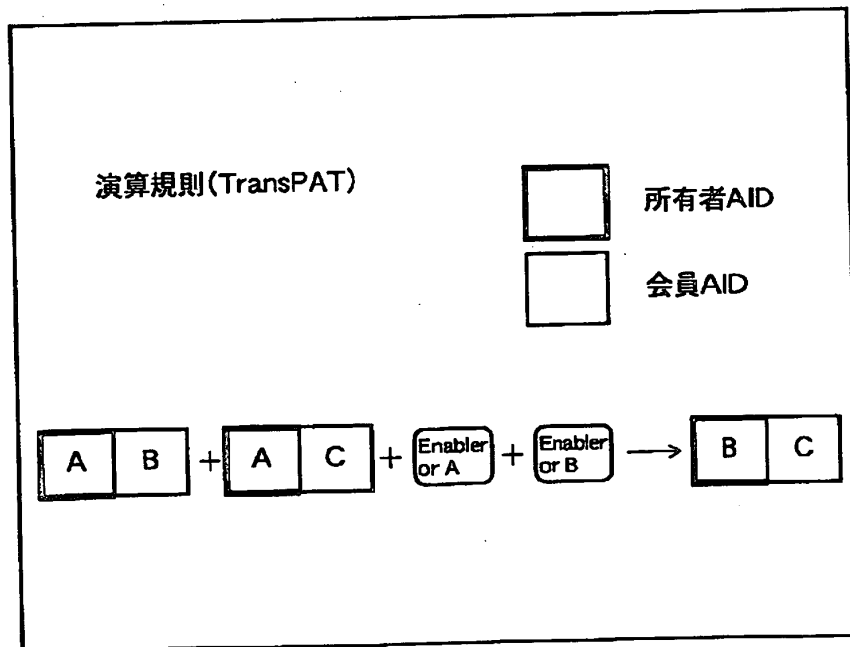
【図 3 4】



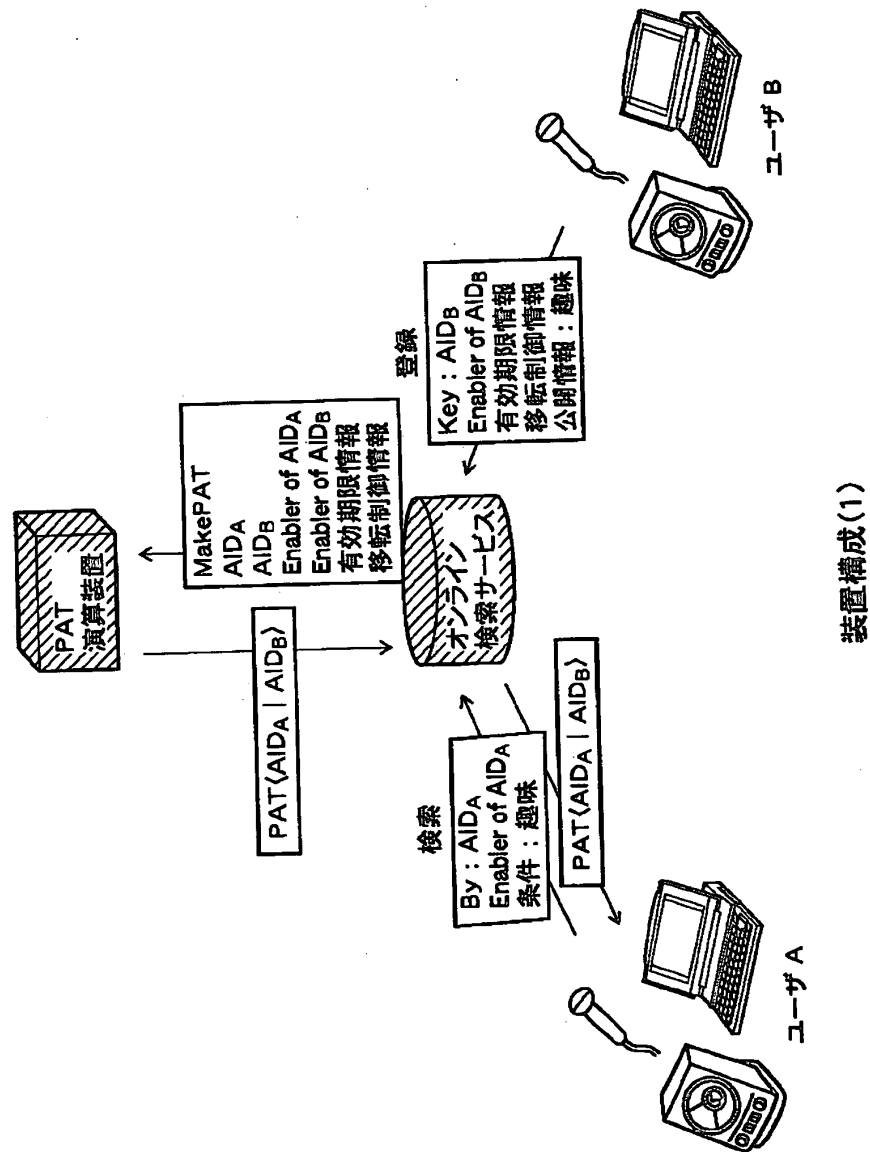
【図 3 5】



【図 3 6】

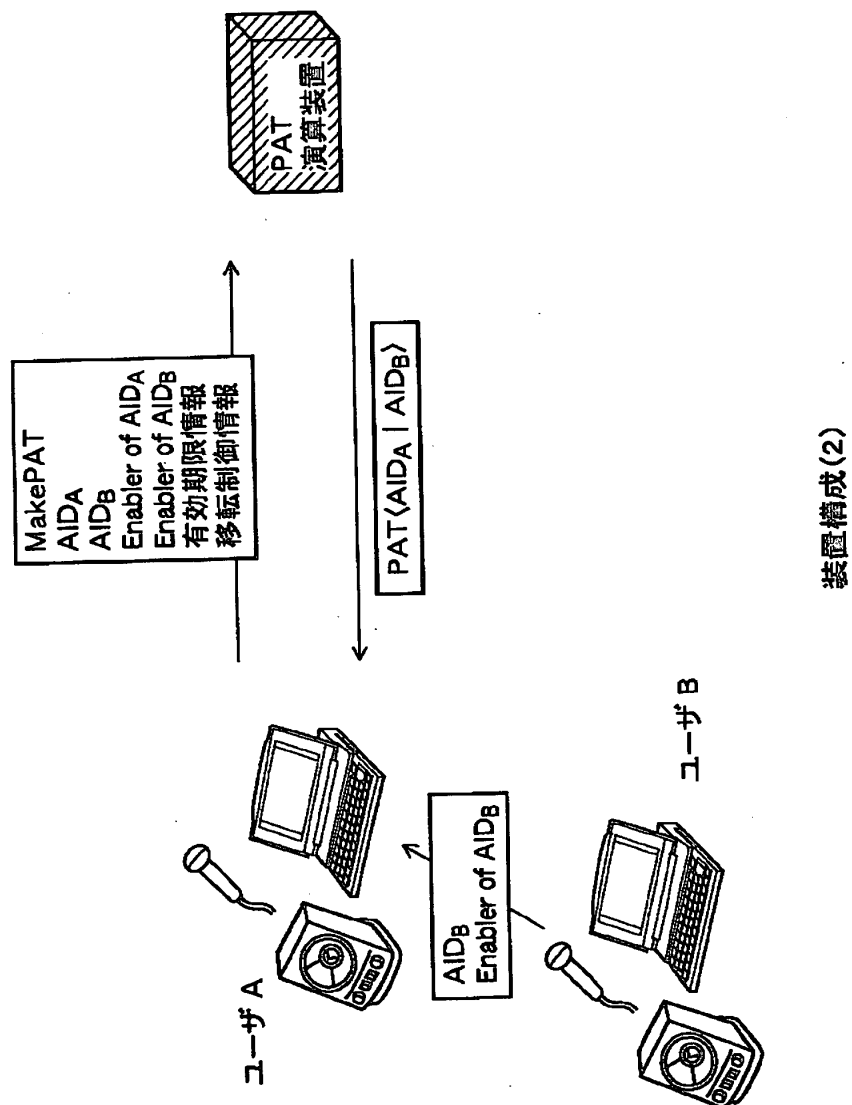


【図37】

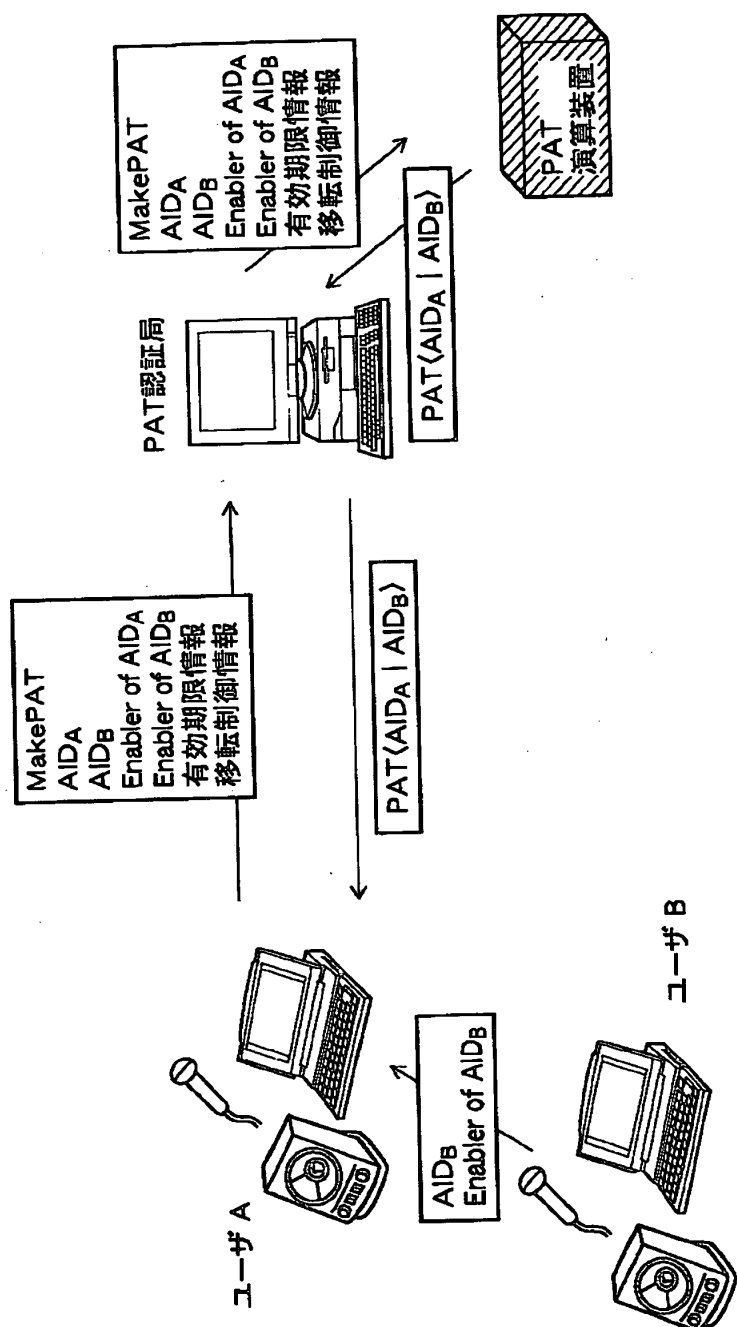


装置構成(1)

【図38】

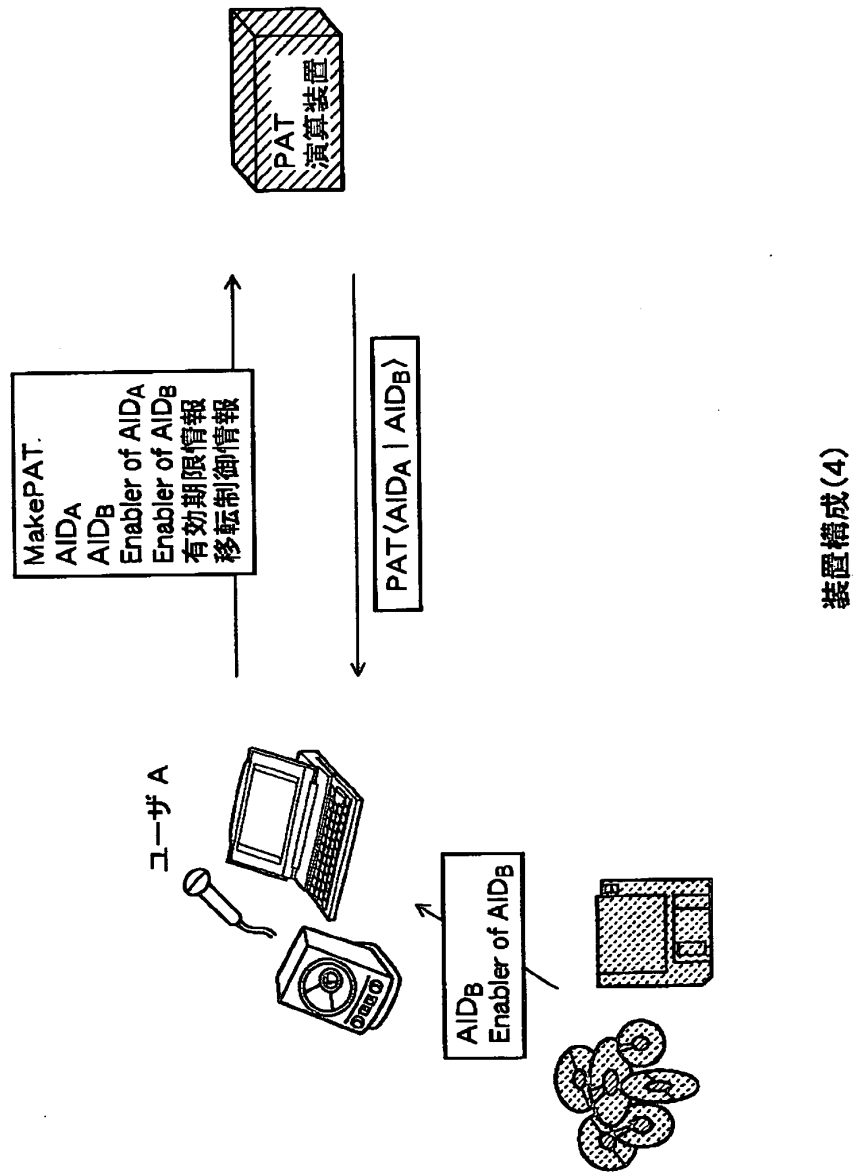


【図 3 9】

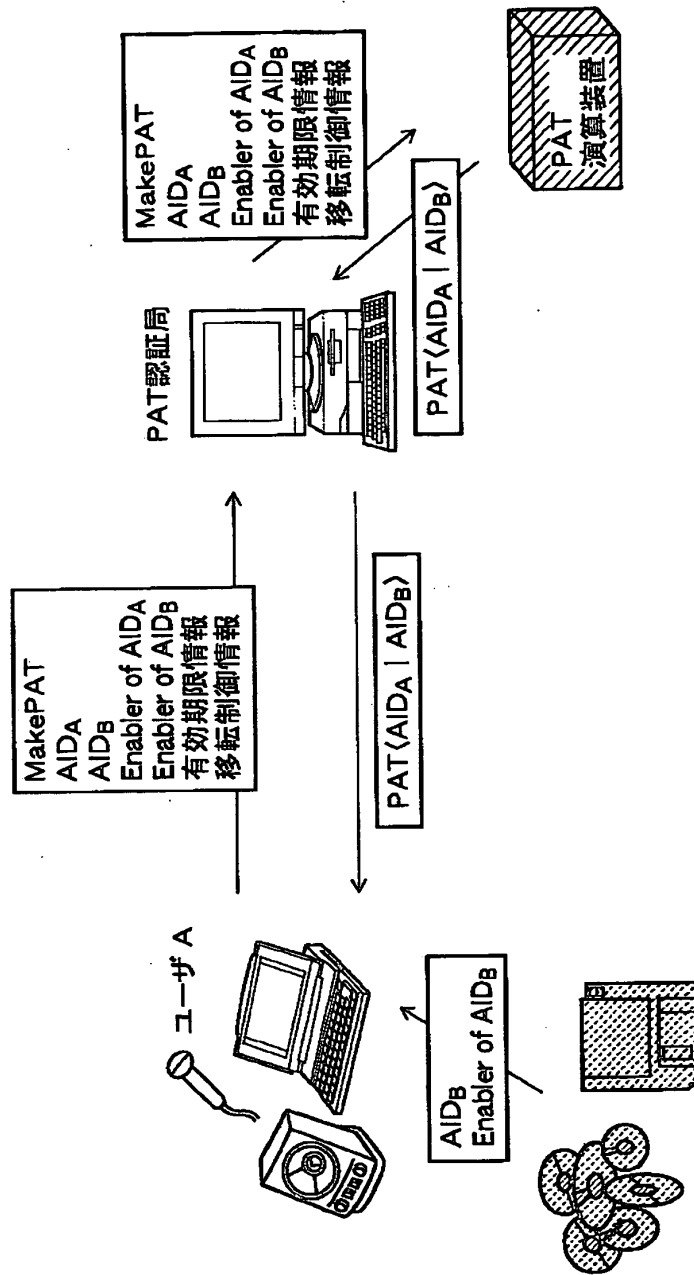


裝置構成(3)

【図 40】

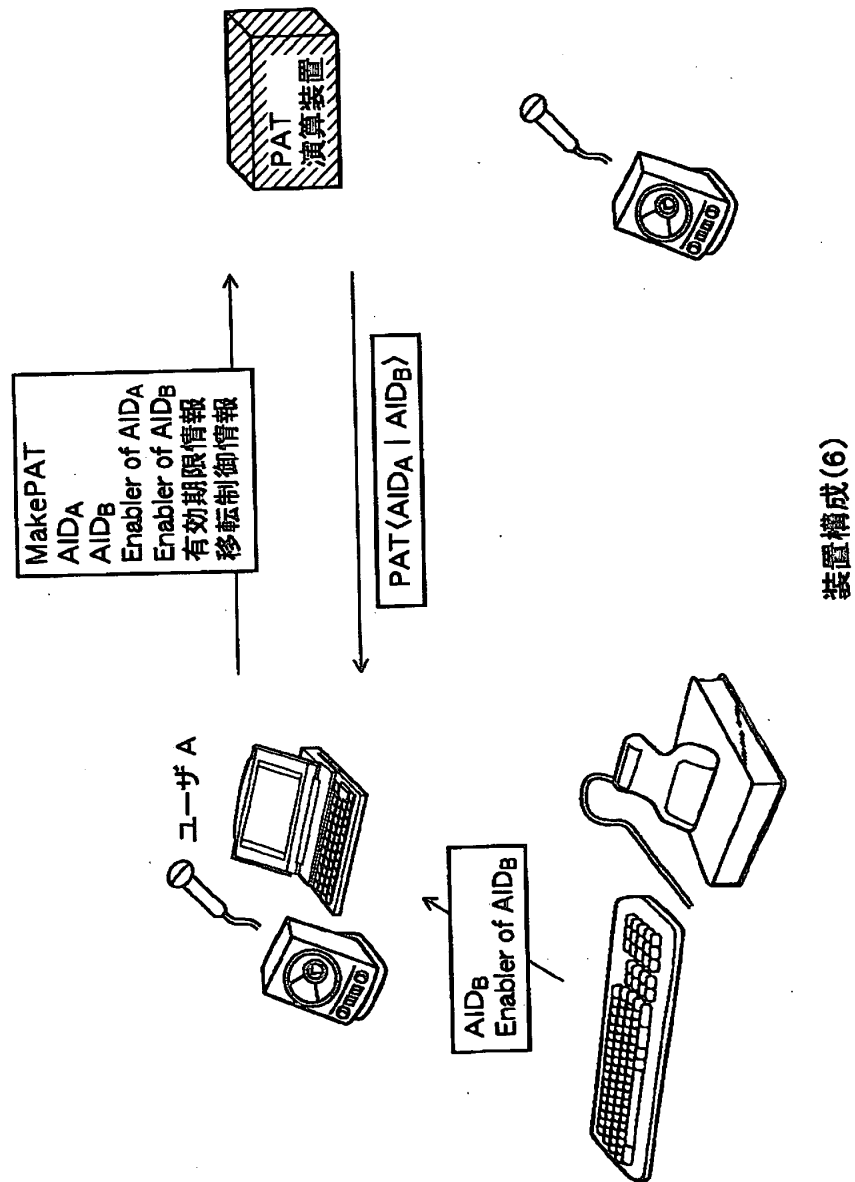


【図41】

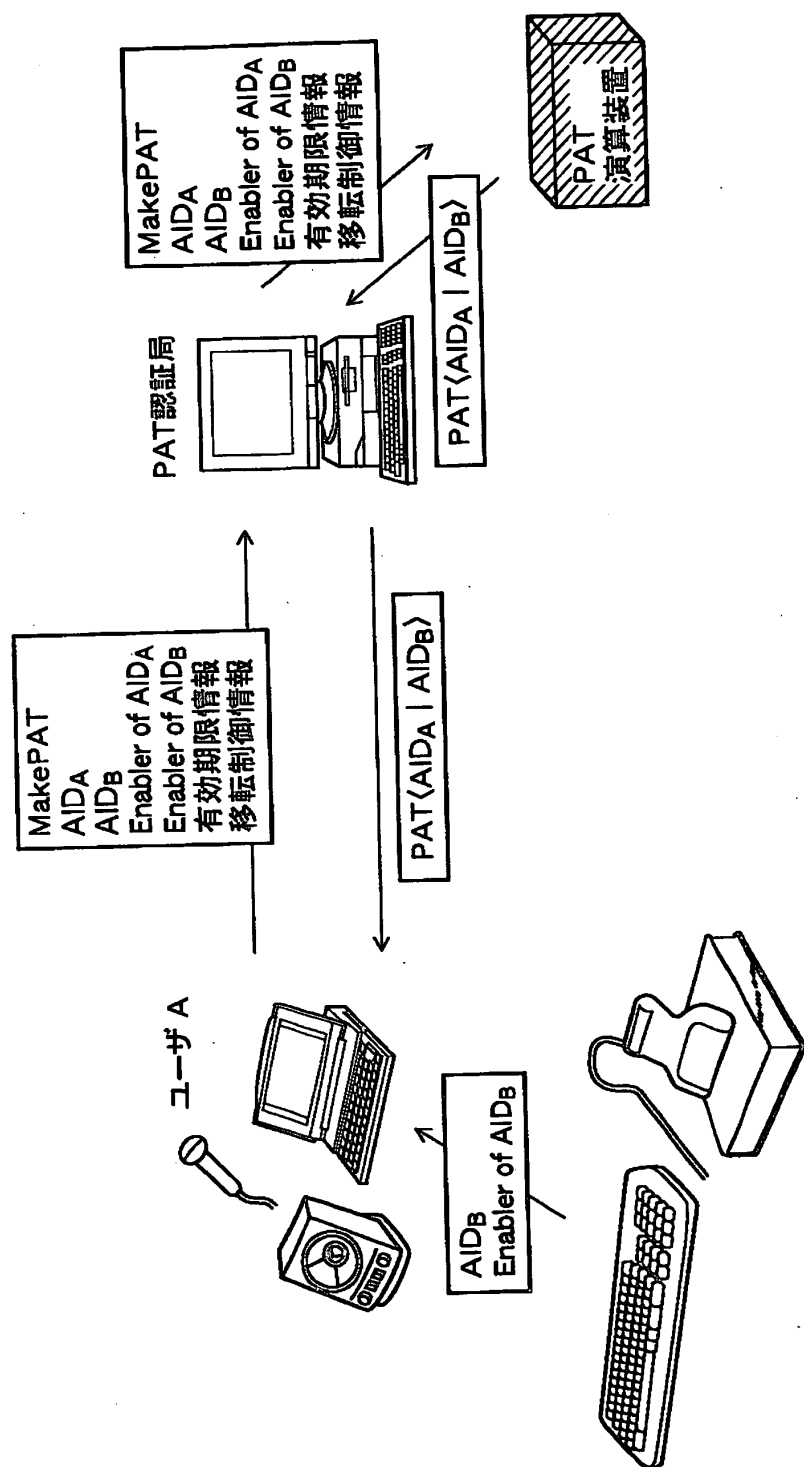


装置構成(5)

【図 4 2】

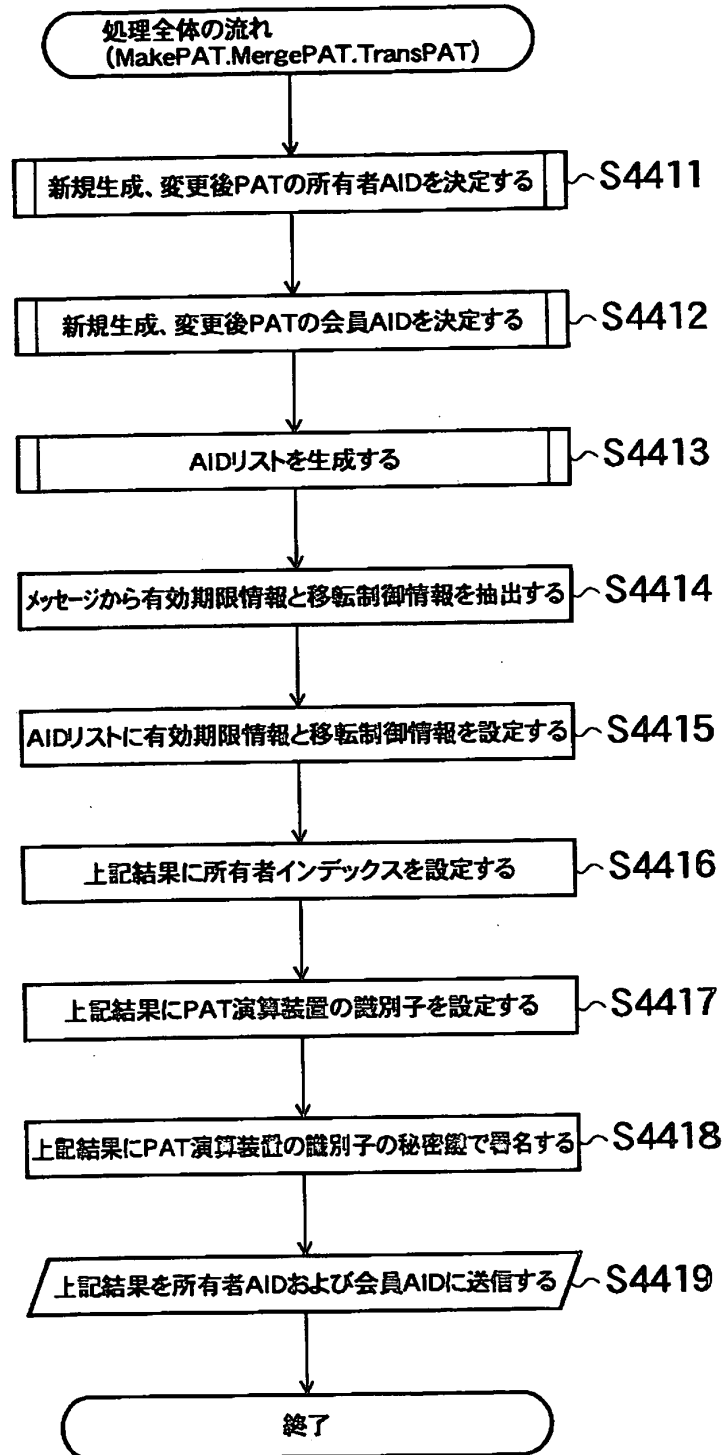


【図 4 3】

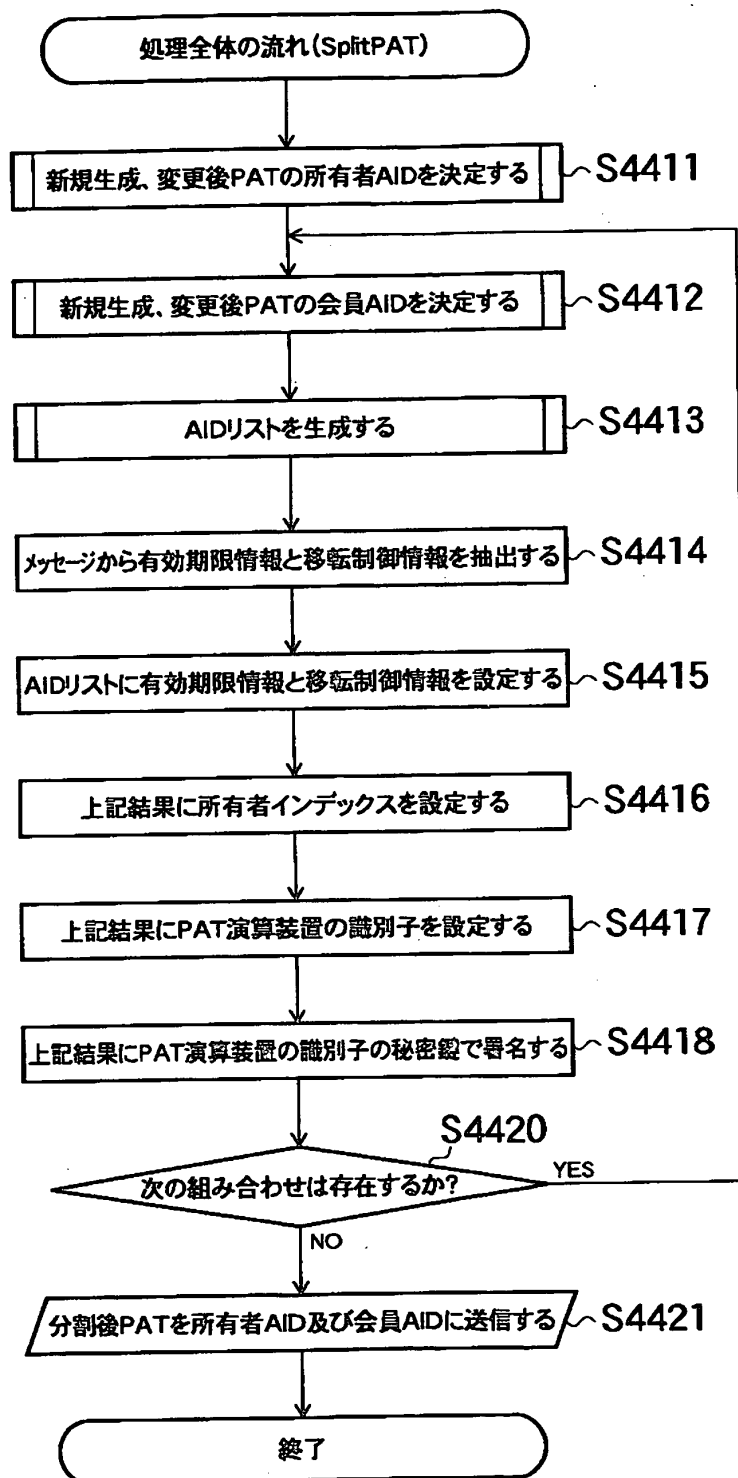


裝置構成(7)

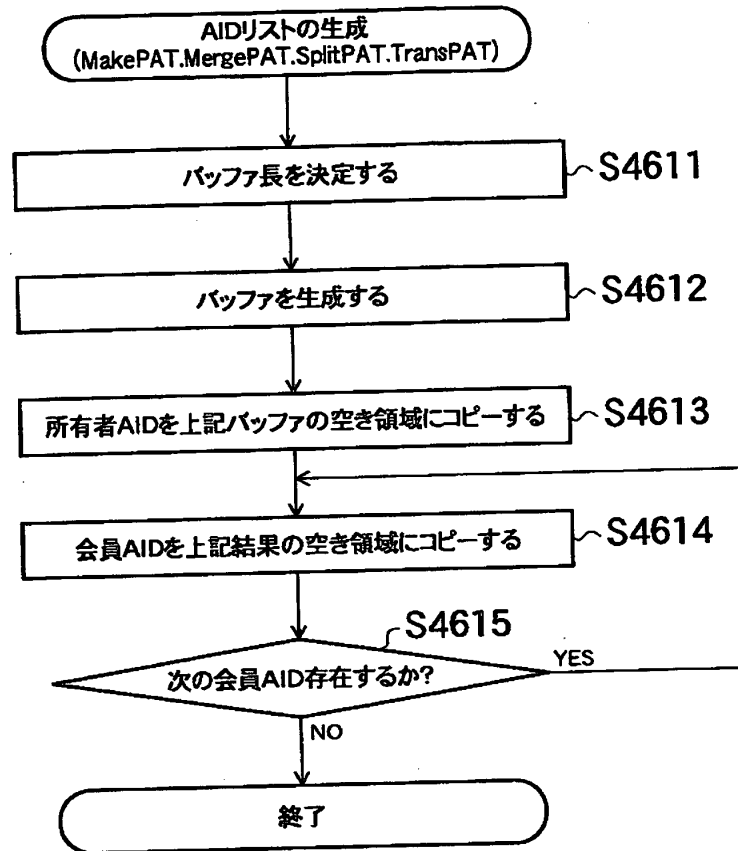
【図 4 4】



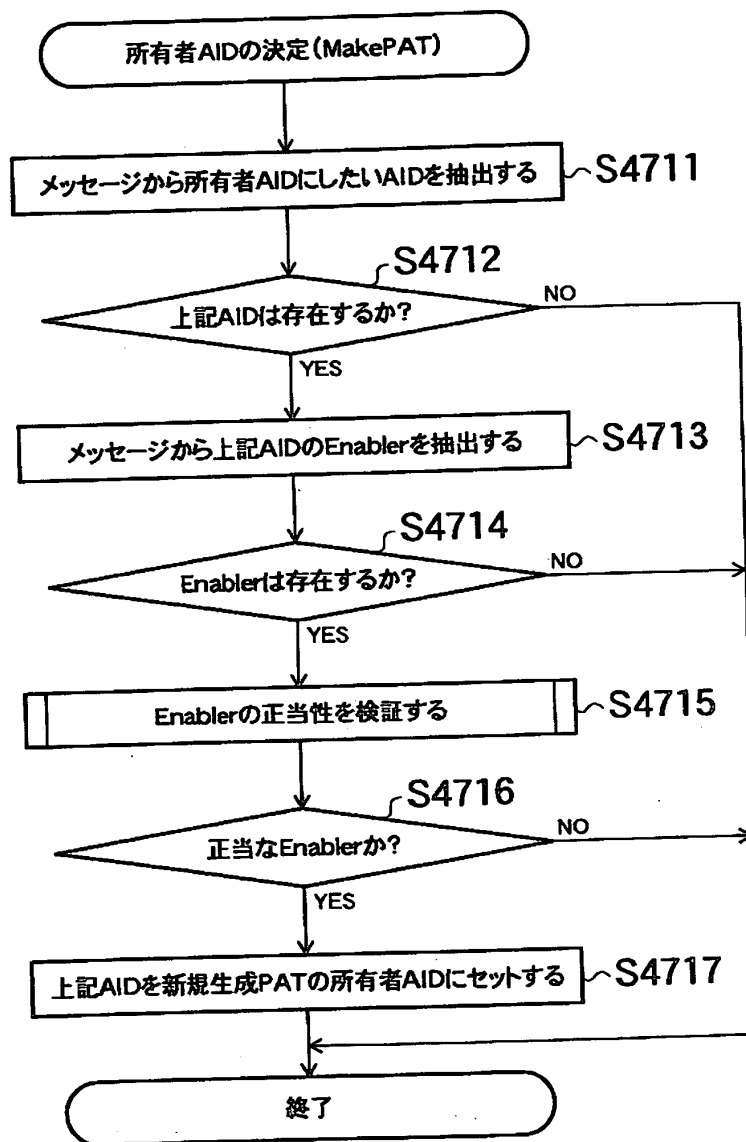
【図 45】



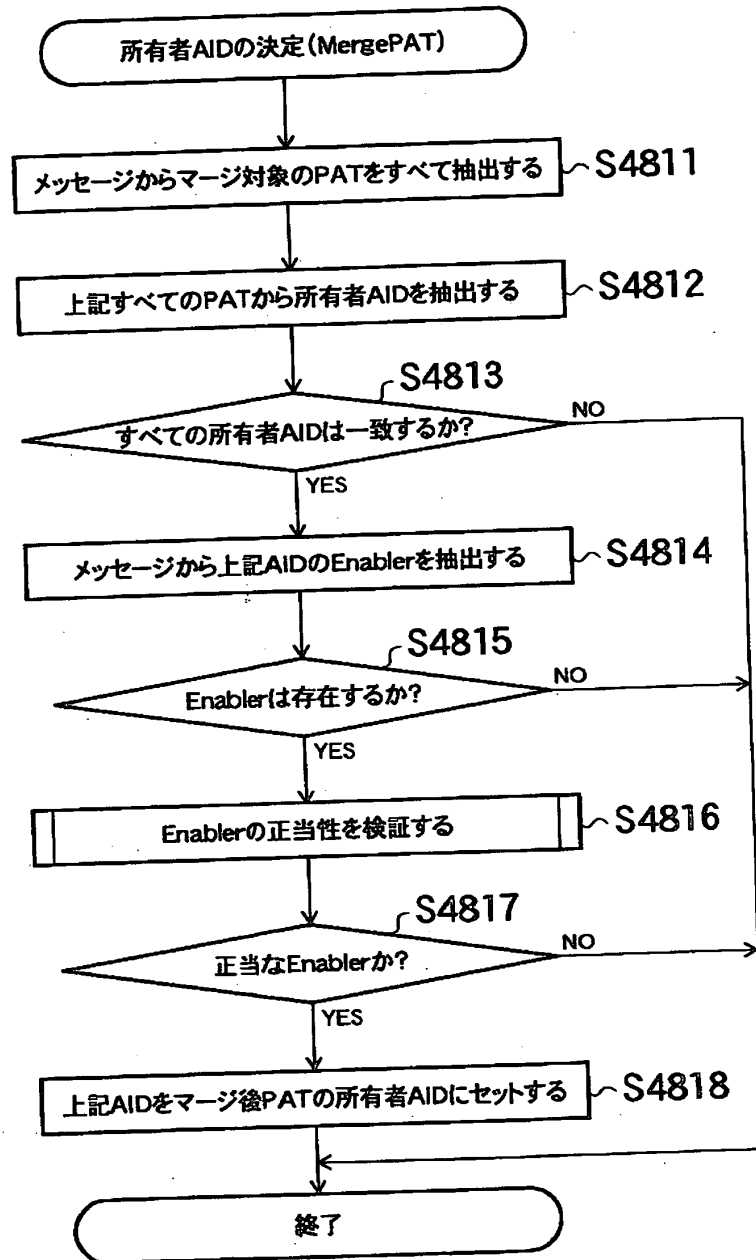
【図 4 6】



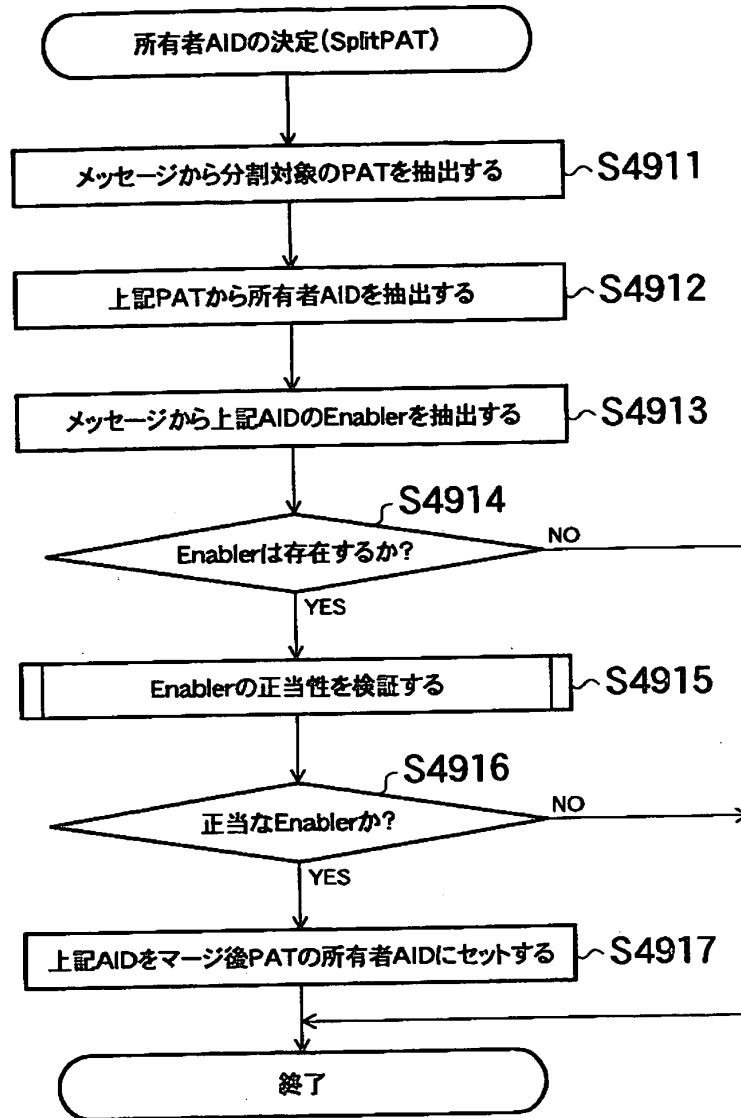
【図 47】



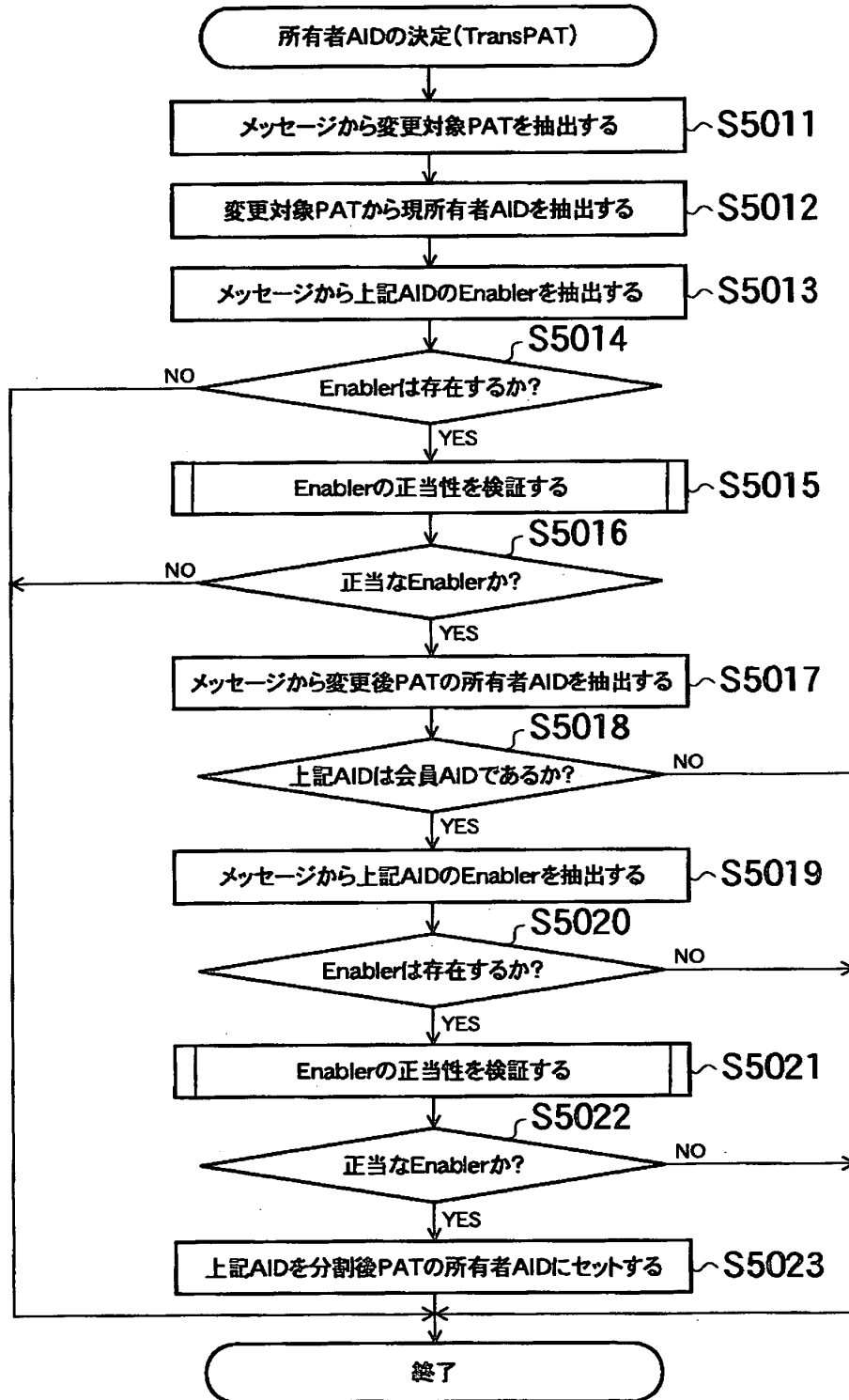
【図48】



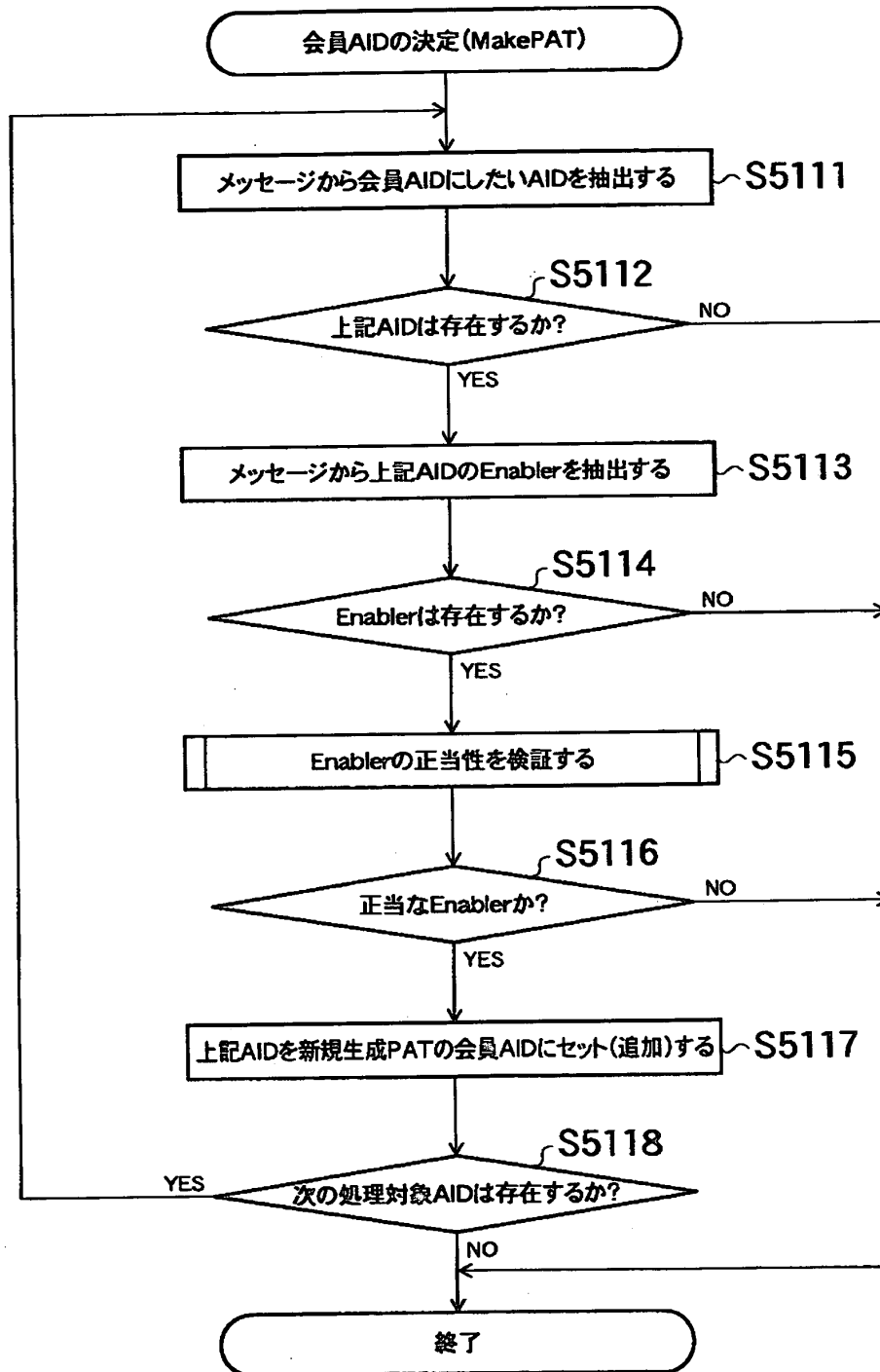
【図 49】



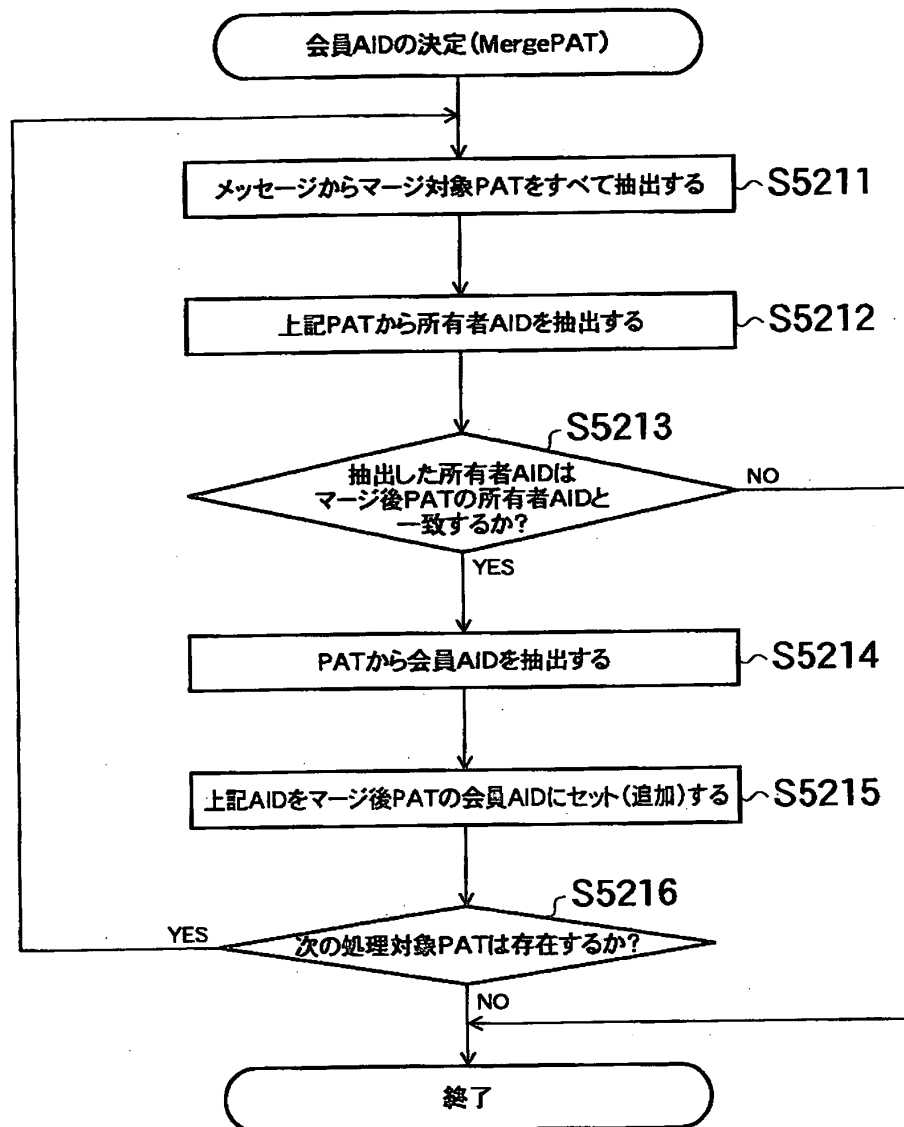
【図 50】



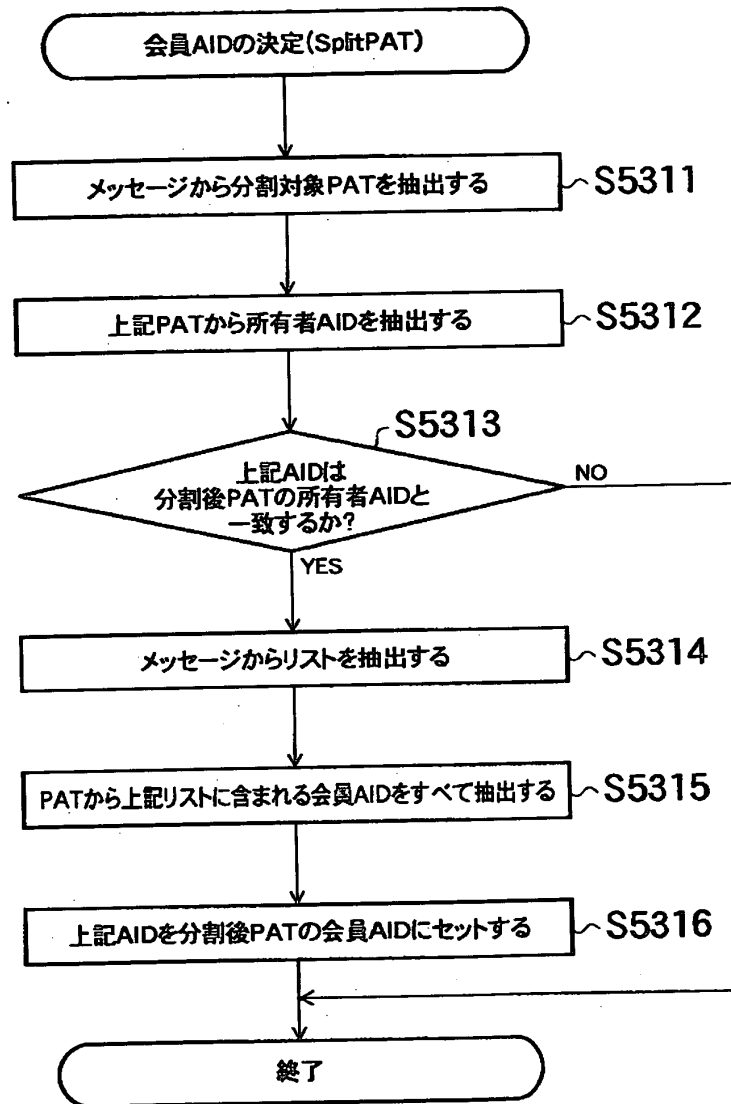
【図51】



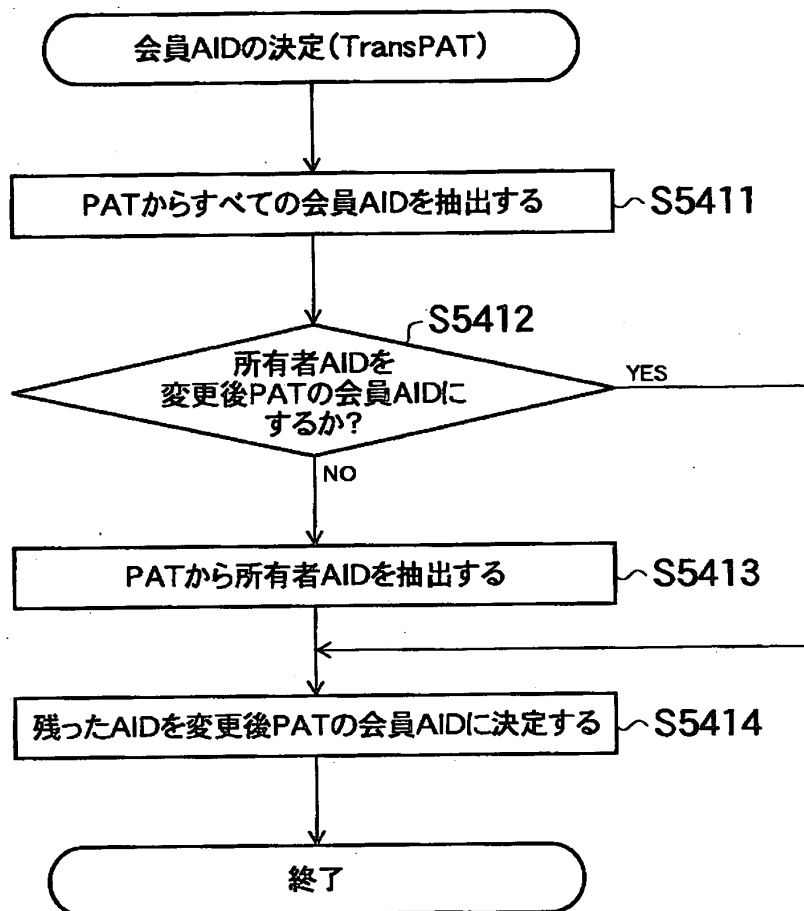
【図 52】



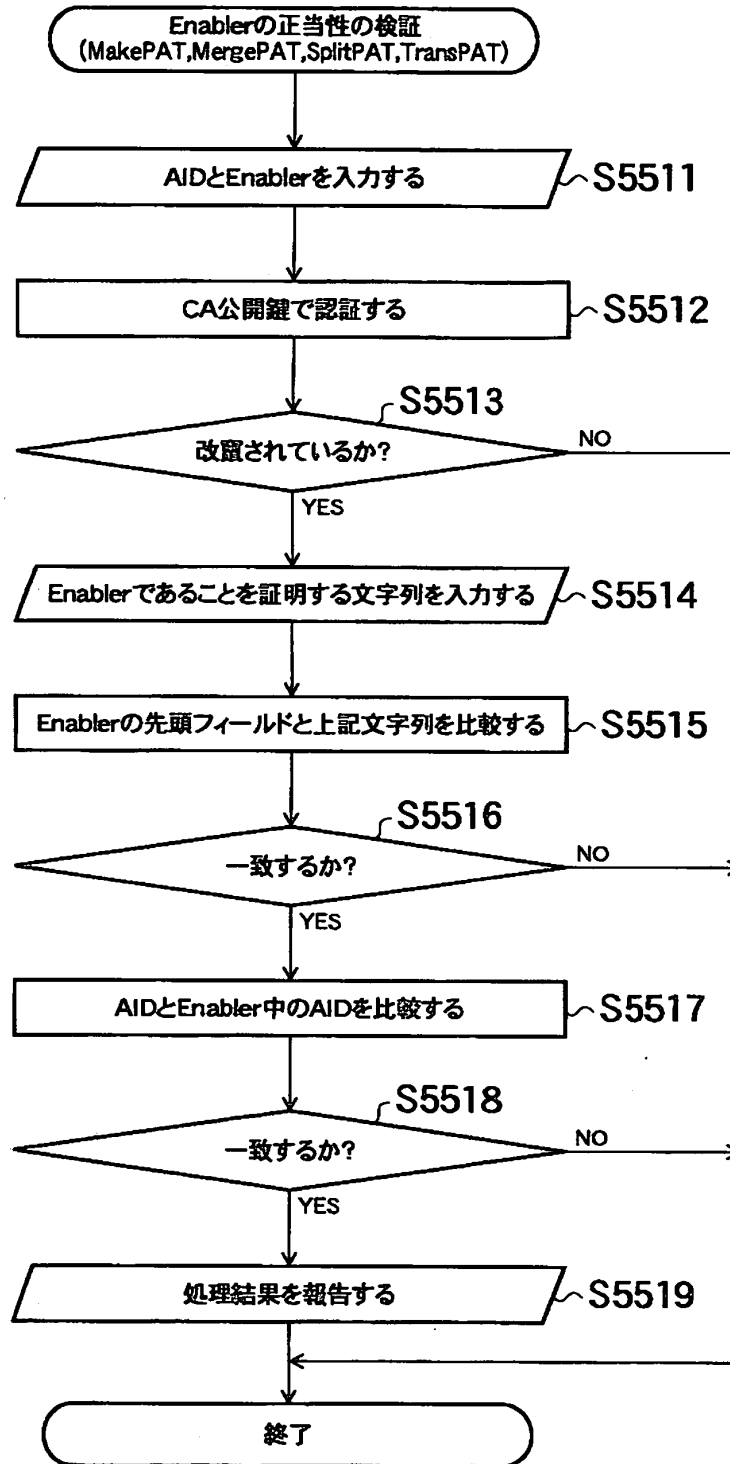
【図 53】



【図 54】



【図 55】



【図56】

MakePAT命令を含むメッセージ

MakePAT	
新規生成PATの所有者AID	左記AIDのEnabler
新規生成PATの会員AID ₁	左記AID ₁ のEnabler
会員AID ₂	左記AID ₂ のEnabler
...	
会員AID _n	左記AID _n のEnabler
有効期限情報	
移転制御情報	

【図 57】

MergePAT命令を含むメッセージ

MergePAT
 マージ対象PAT <所有者AID | 会員AID₁₁, 会員AID₁₂... 会員AID_{1n}>
 マージ対象PAT <所有者AID | 会員AID₂₁, 会員AID₂₂... 会員AID_{2n}>
 ...
 マージ対象PAT <所有者AID | 会員AID_{m1}, 会員AID_{m2}... 会員AID_{mn}>
 マージ後PATの所有者AIDのEnabler
 有効期限情報
 移転制御情報

【図 58】

SplitPAT命令を含むメッセージ

SplitPAT
 分割対象PAT <所有者AID | 会員AID₁, 会員AID₂... 会員AID_n>
 組み合わせ₁ (会員AID₁, 会員AID₃, 有効期限情報₁, 移転制御情報₁)
 組み合わせ₂ (会員AID₂, 会員AID₅, 有効期限情報₂, 移転制御情報₂)
 ...
 組み合わせ_n (会員AID_k, 会員AID_l, 有効期限情報_n, 移転制御情報_n)
 分割後PATの所有者AIDのEnabler

【図 59】

TransPAT命令を含むメッセージ

TransPAT

所有者権変更対象PAT <所有者AID | 会員AID₁, 会員AID₂, ... 会員AID_n>

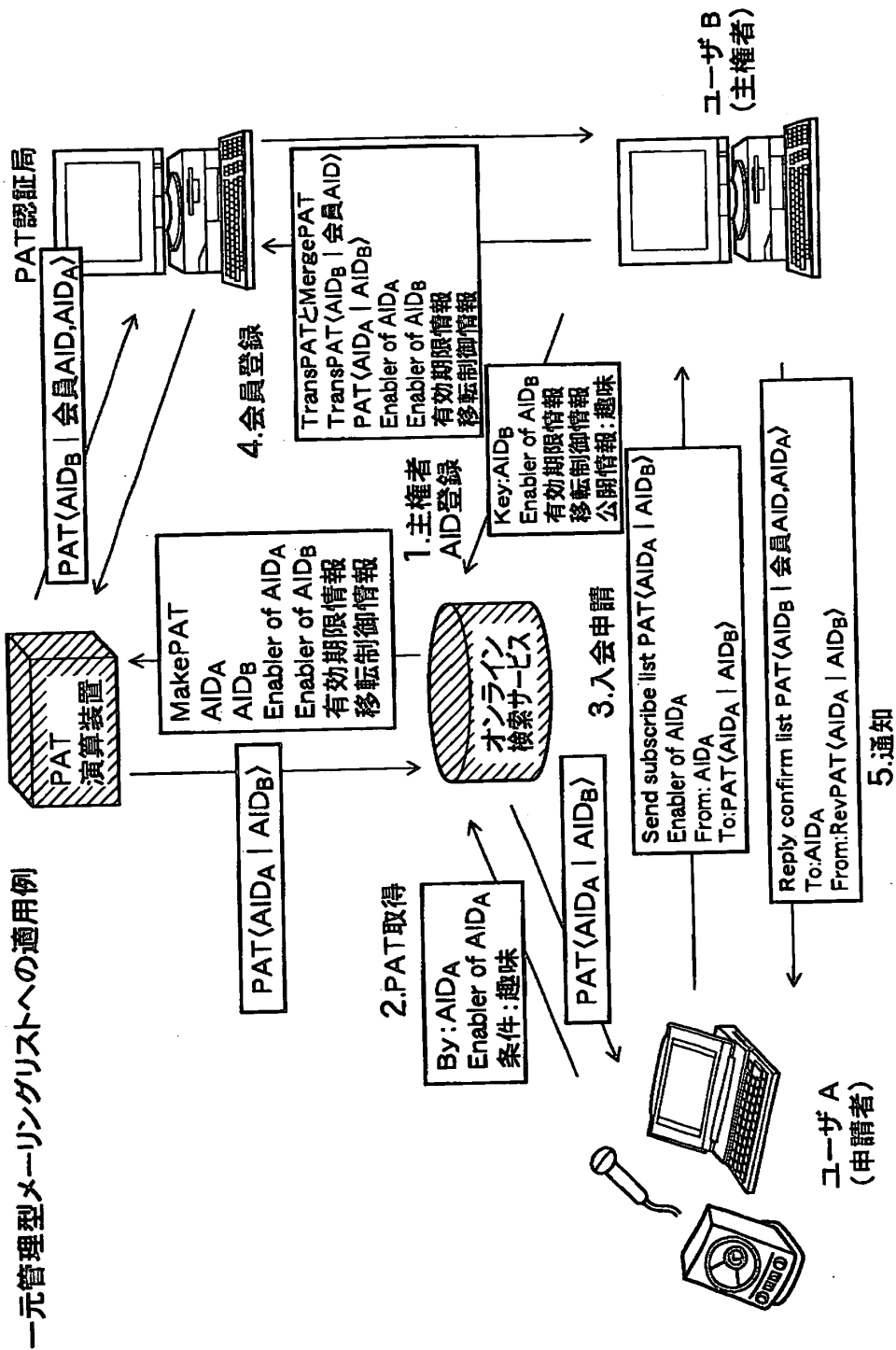
所有者AIDのEnabler

所有者権変更後PATの所有者AID 左記AIDのEnabler

有効期限情報

移転制御情報

【図60】



【図 61】

Null-AID のデータ構造

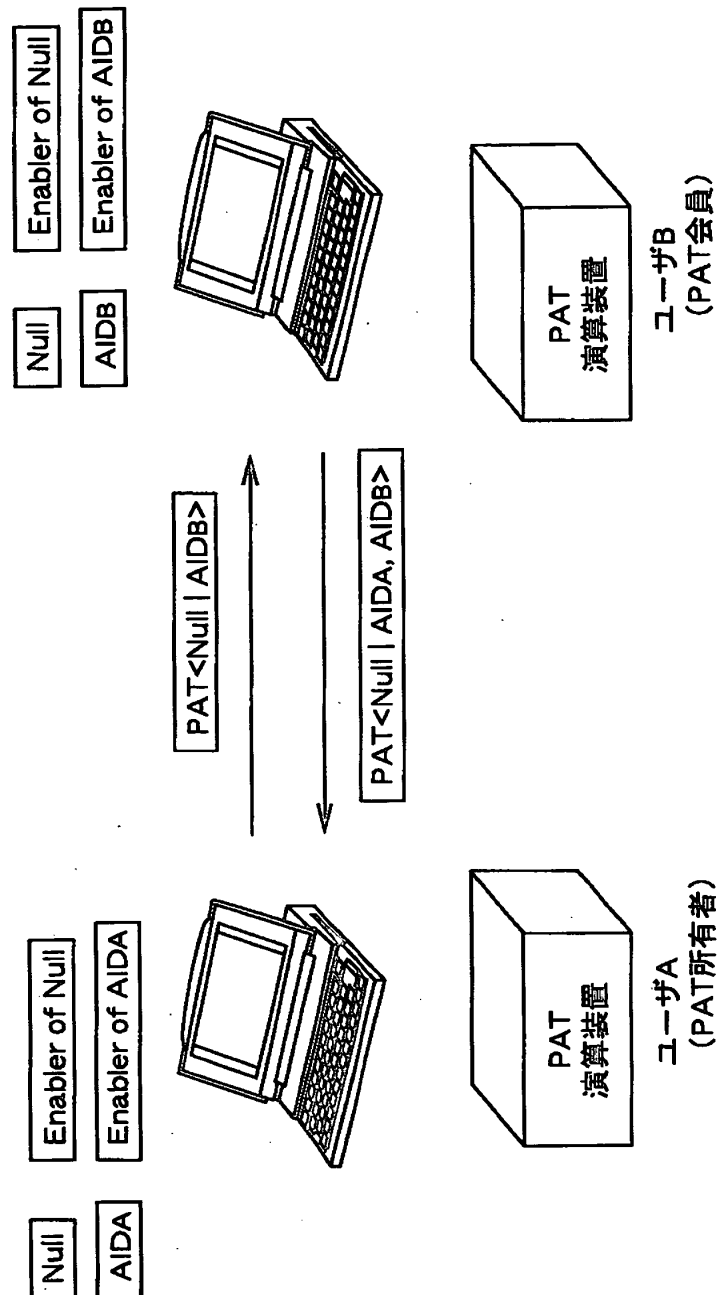
Null-AIDであることを一意に表す文字列	CA署名
------------------------	------

【図 6 2】

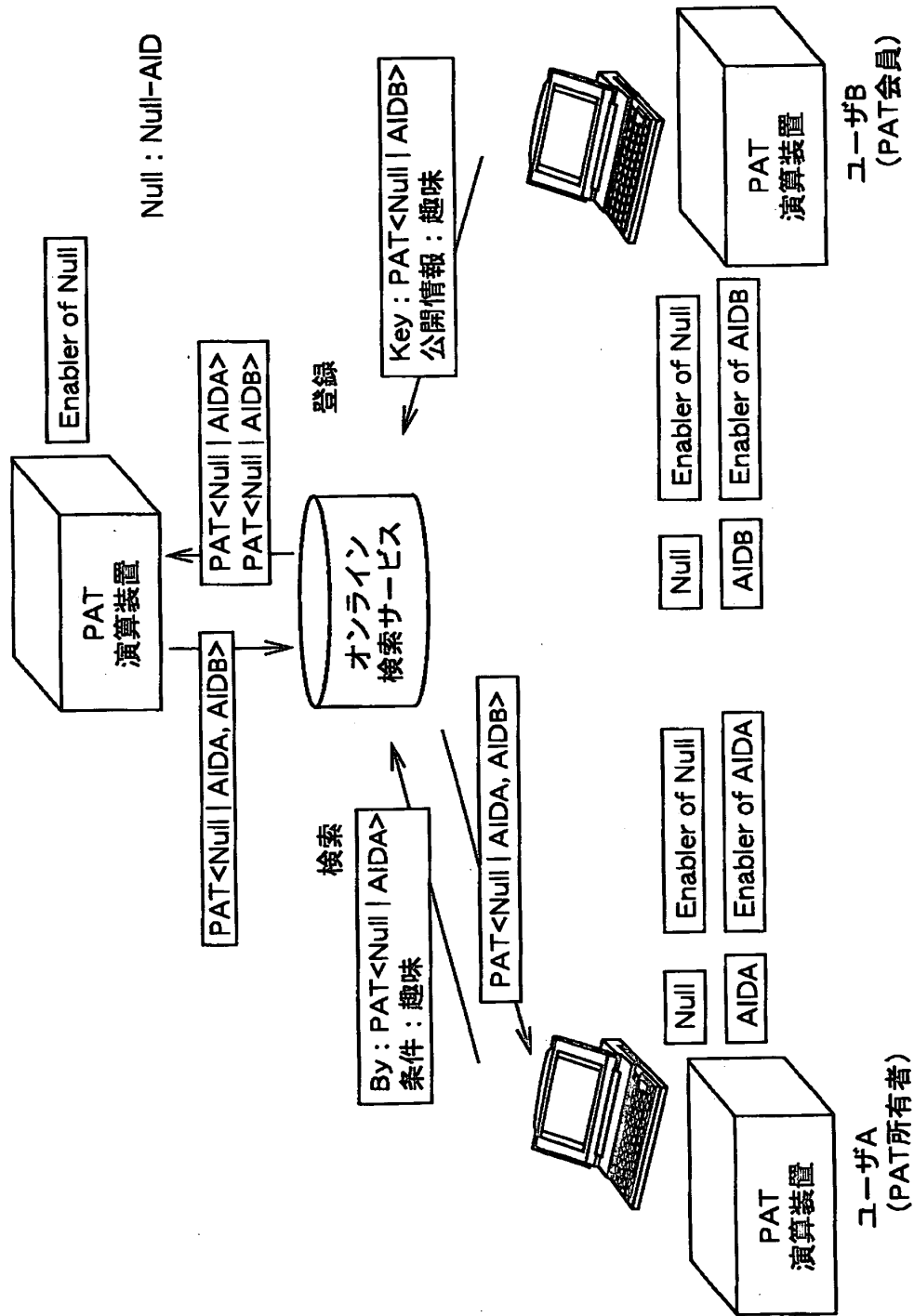
Enabler of Null-AID のデータ構造

Enabler であることを 一意に表す文字列	Null-AID の実体	CA 署名
----------------------------	--------------	-------

【図 63】



【図64】

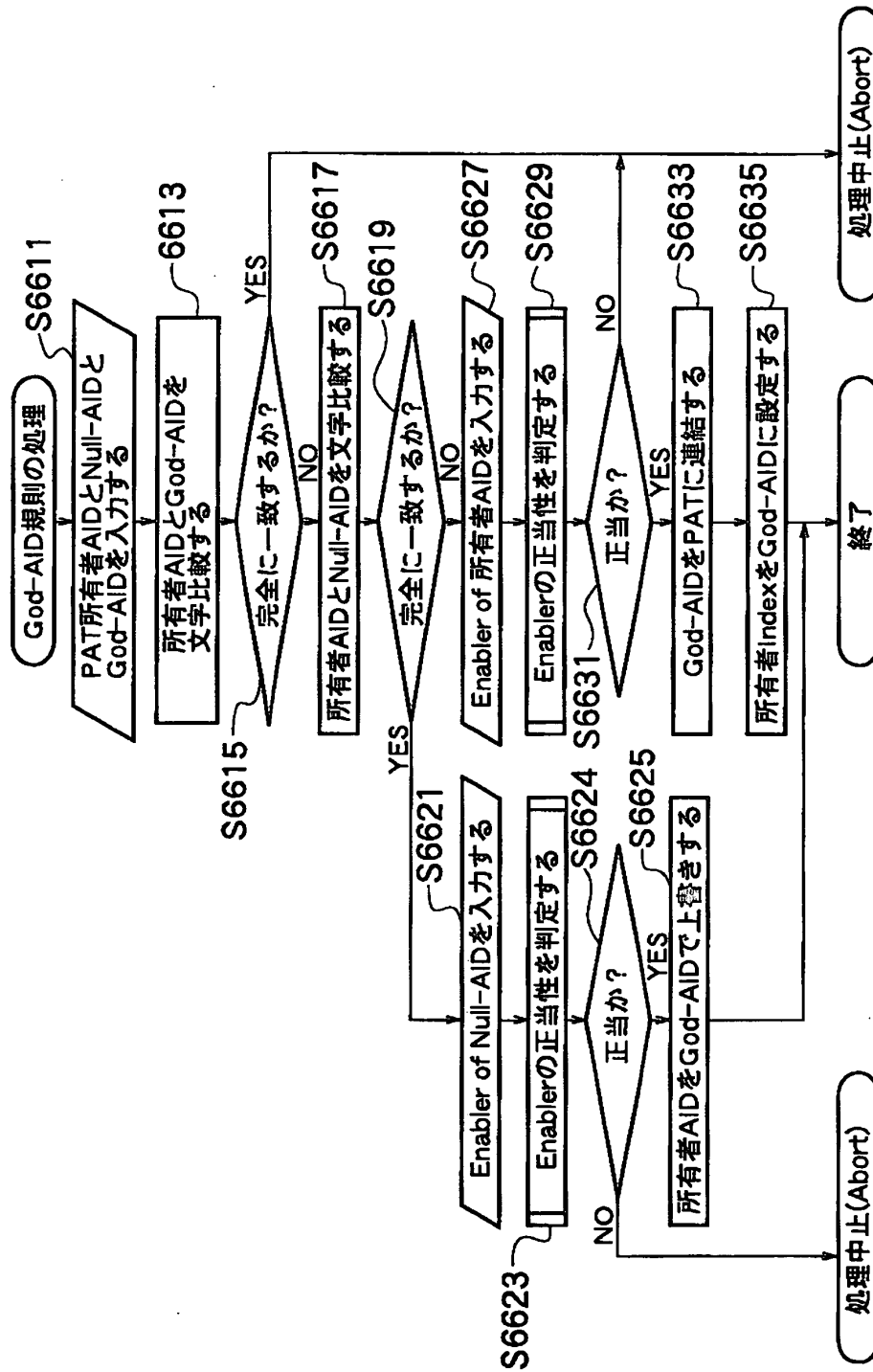


【図 65】

God-AIDのデータ構造

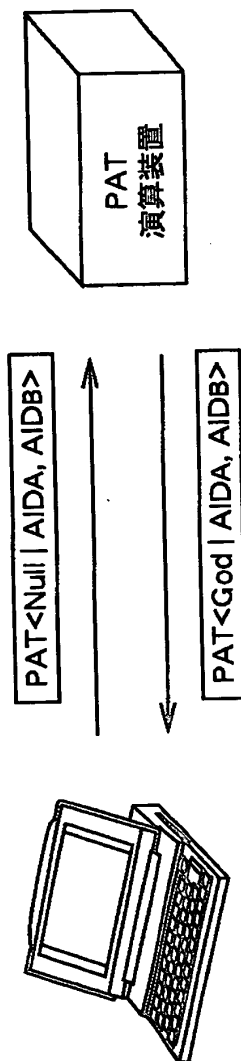
God-AIDであることを一意に表す文字列	CA署名
-----------------------	------

【図 66】

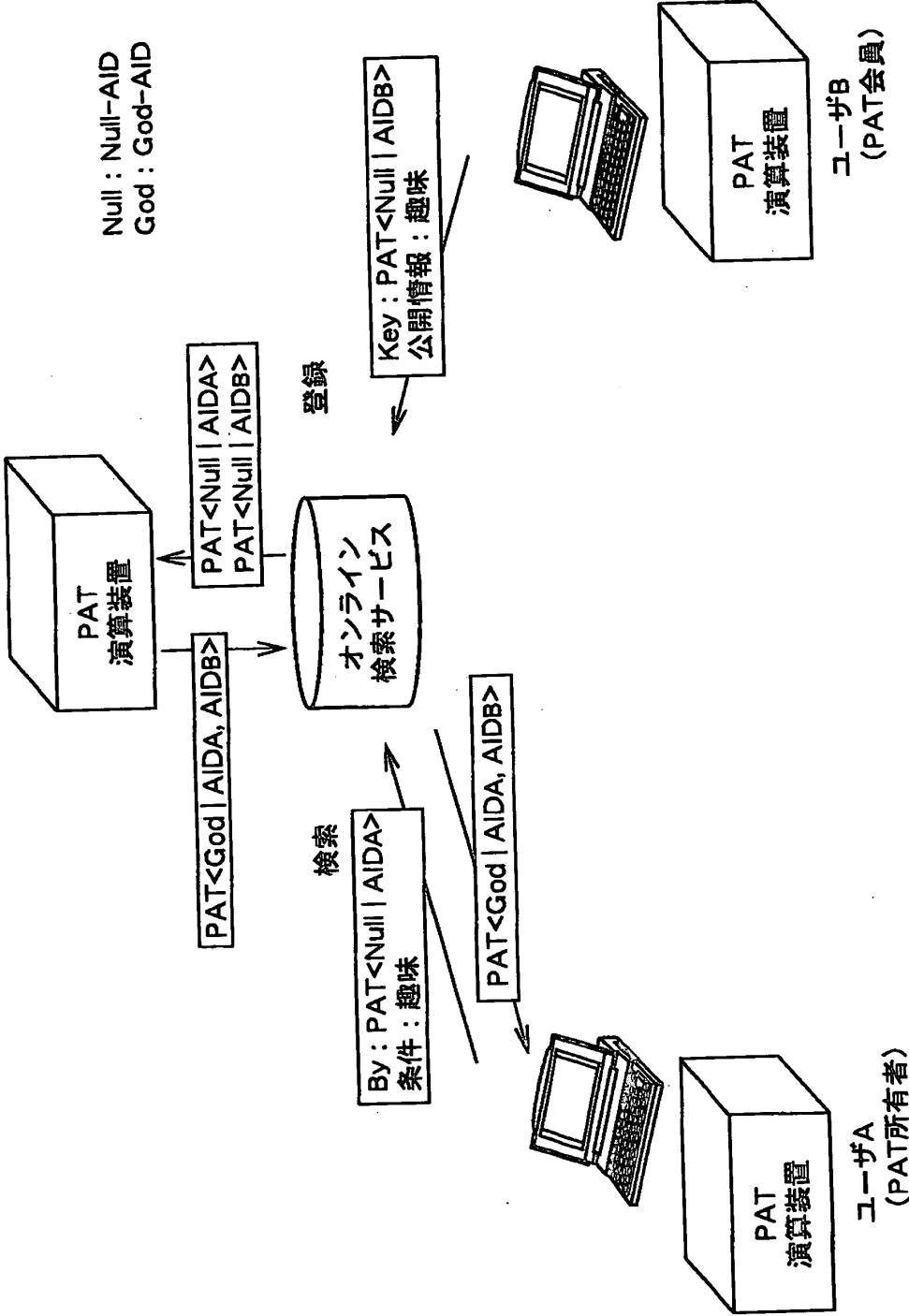


【図 67】

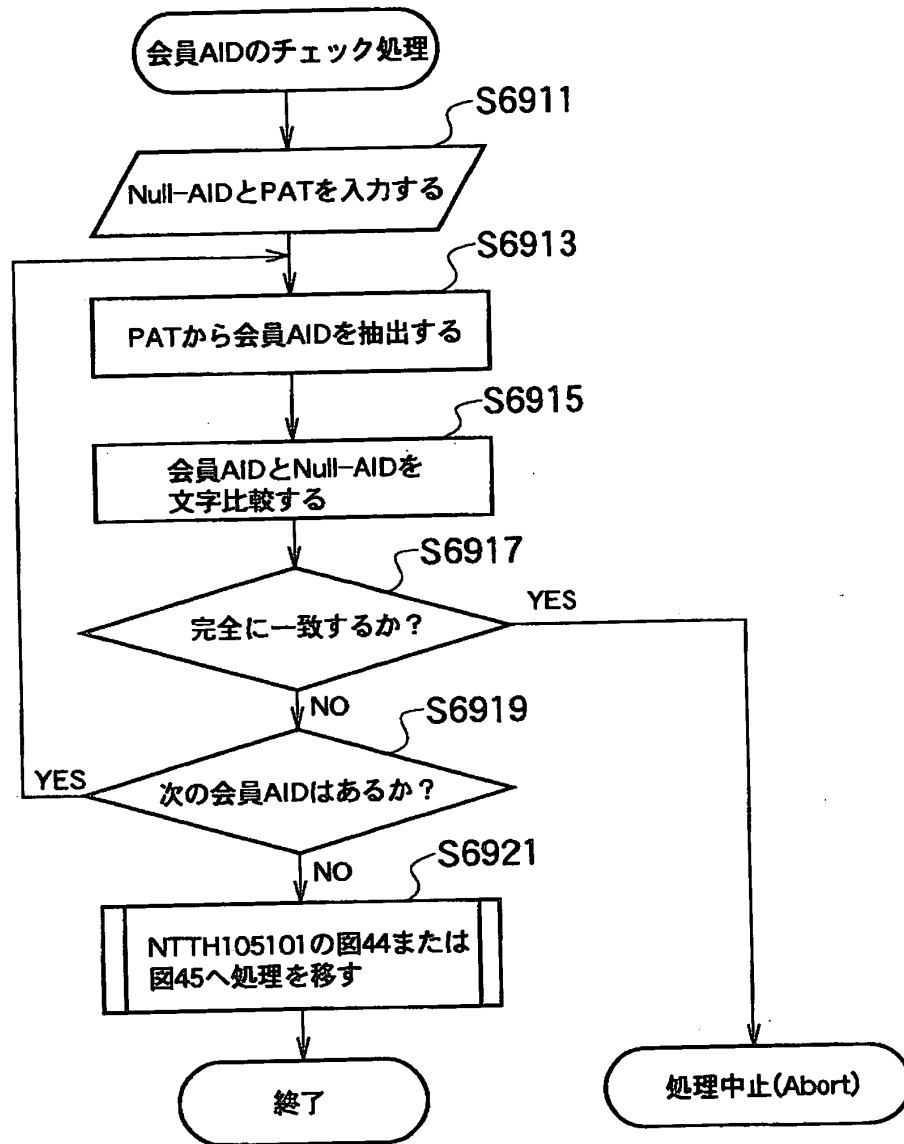
Null : Null-AID
God : God-AID



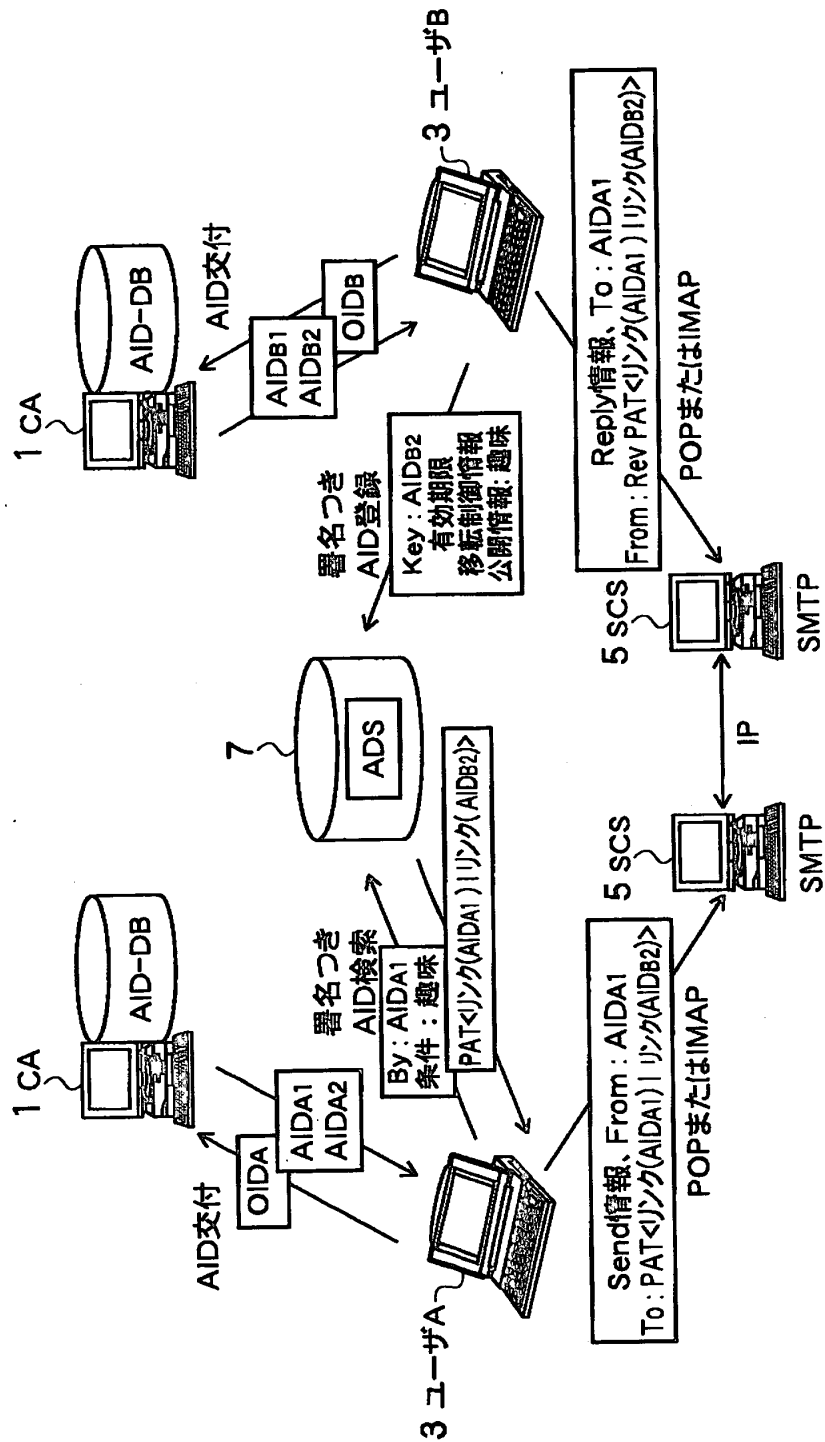
【図68】



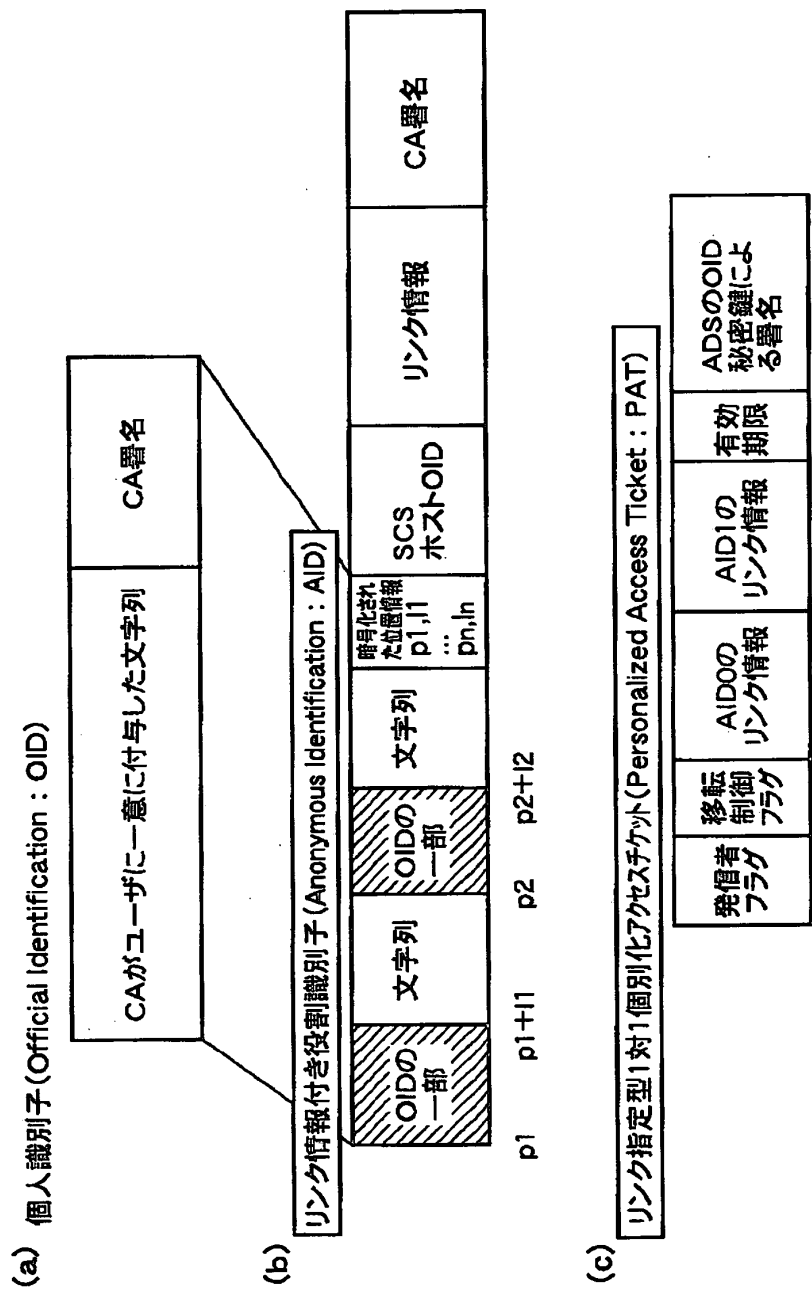
【図 69】



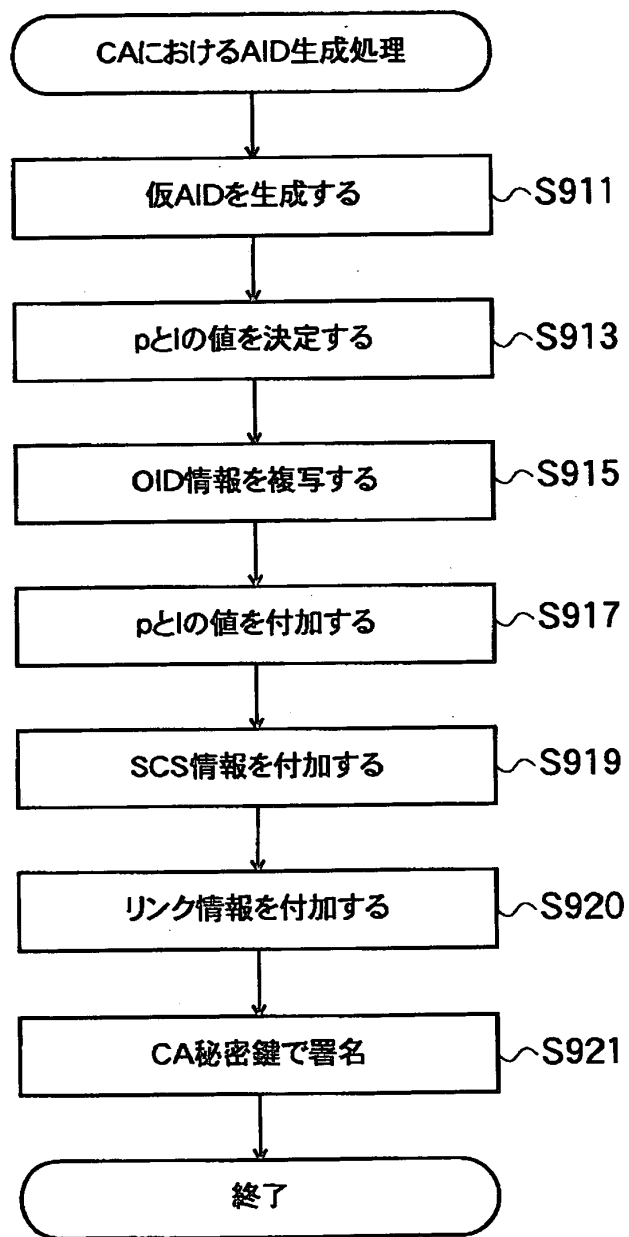
【図70】



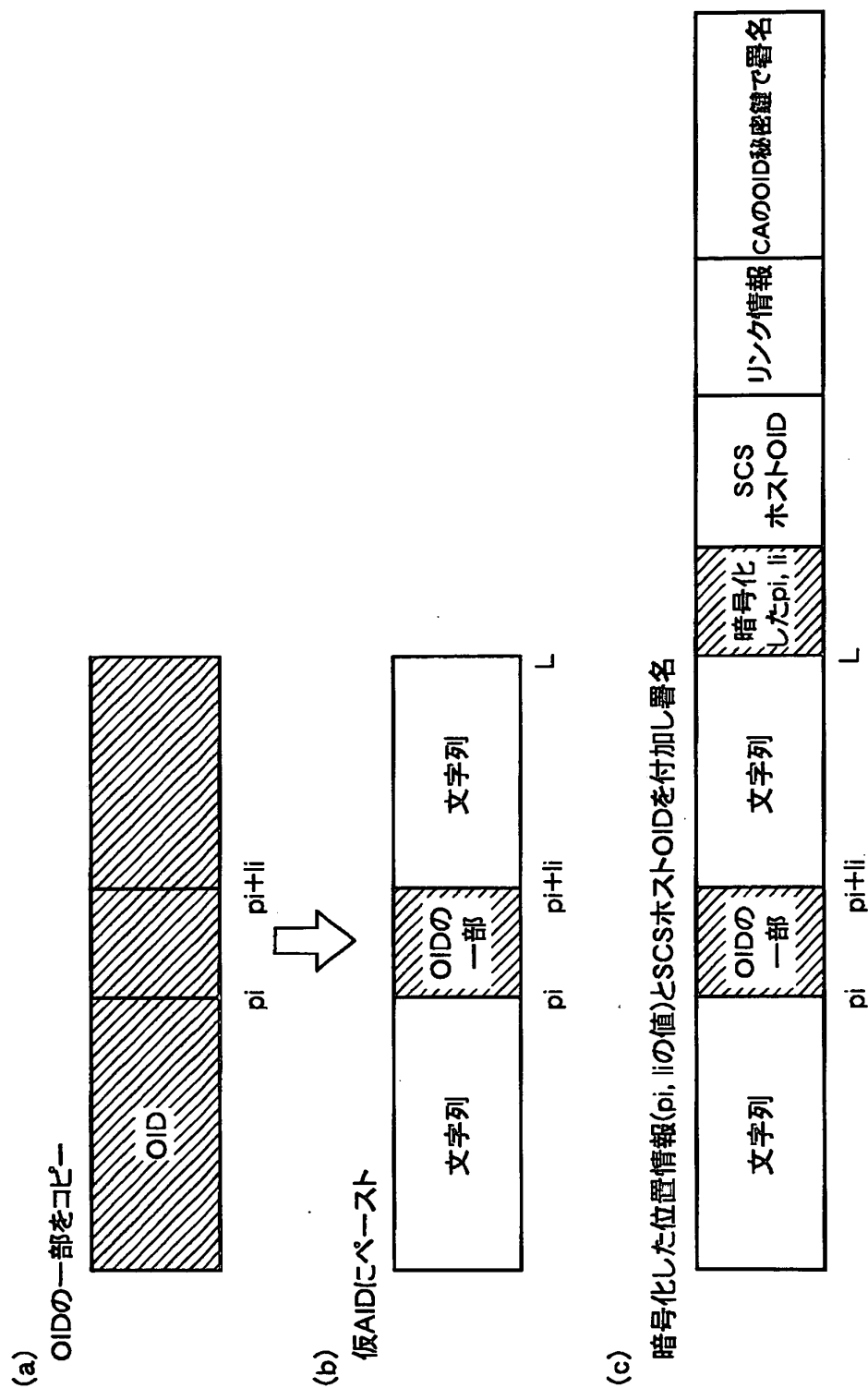
【図 71】



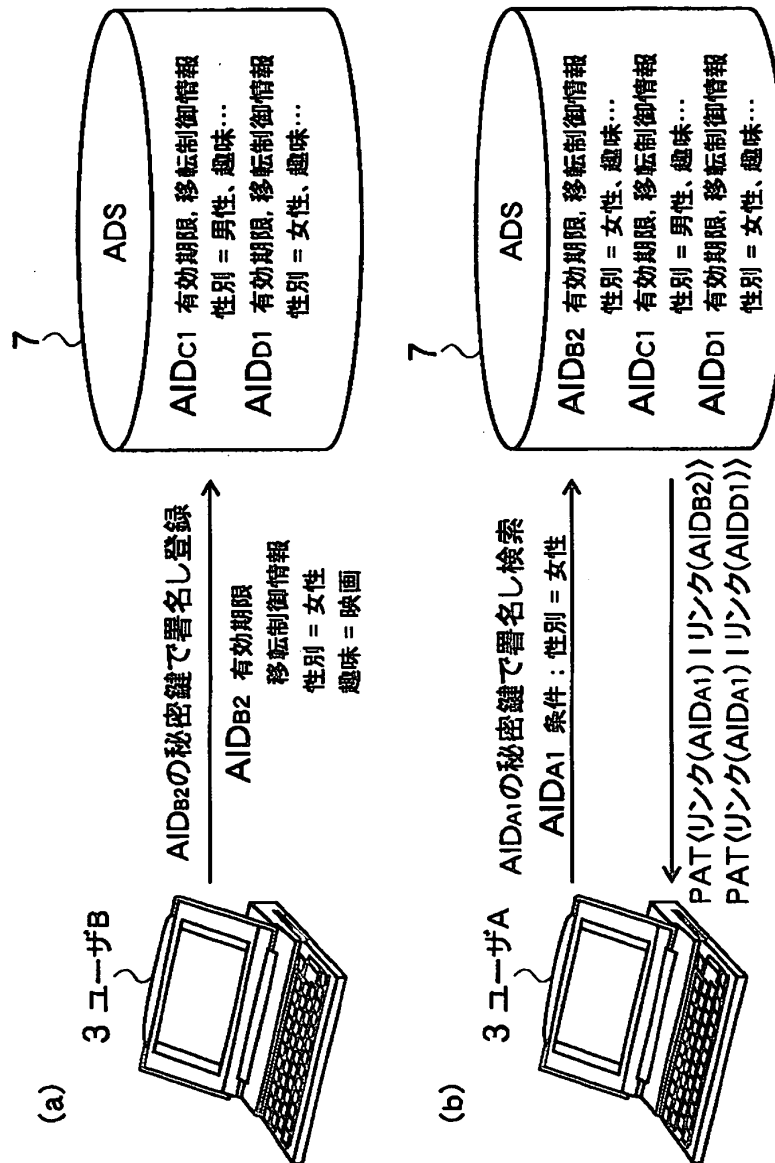
【図 72】



【図73】

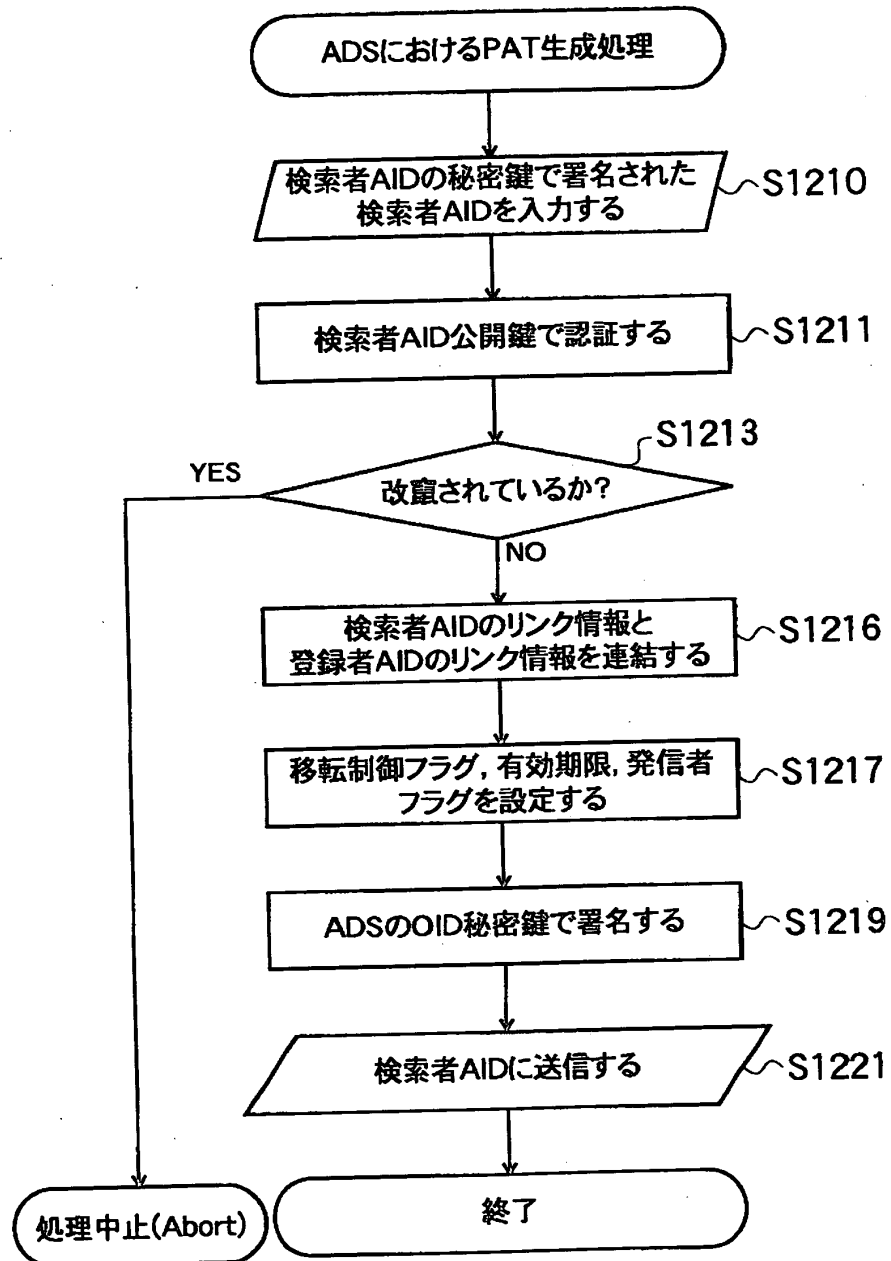


【図 74】

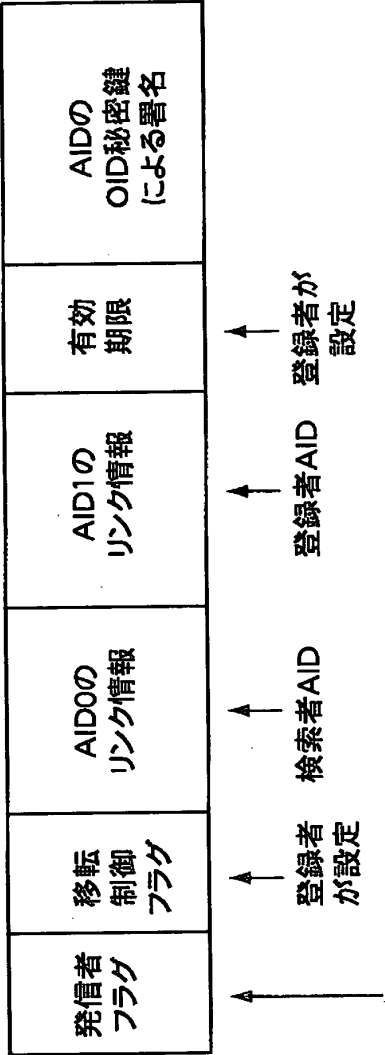


ADSにおけるAID登録とPAT交付の例

【図 75】

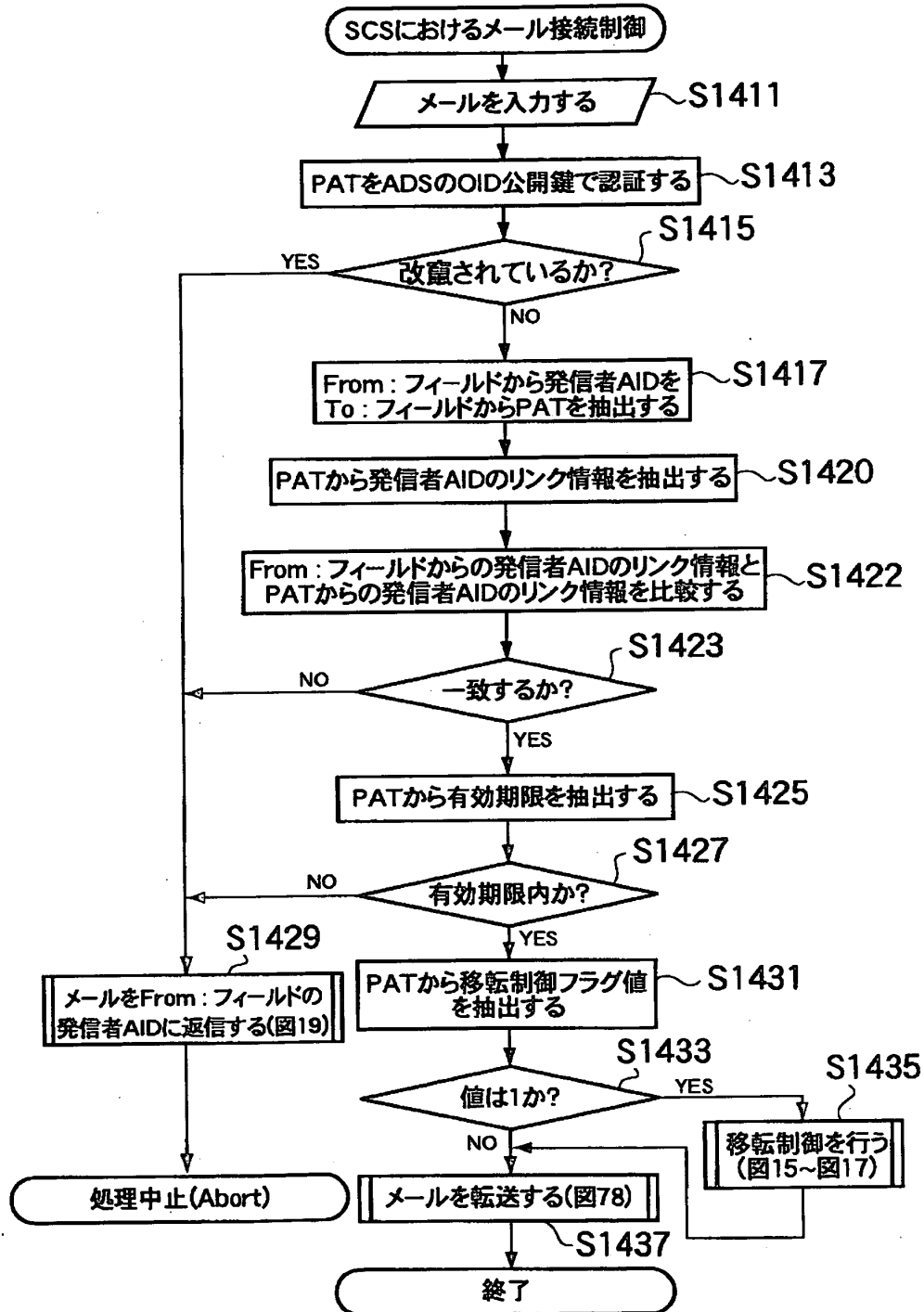


【図76】

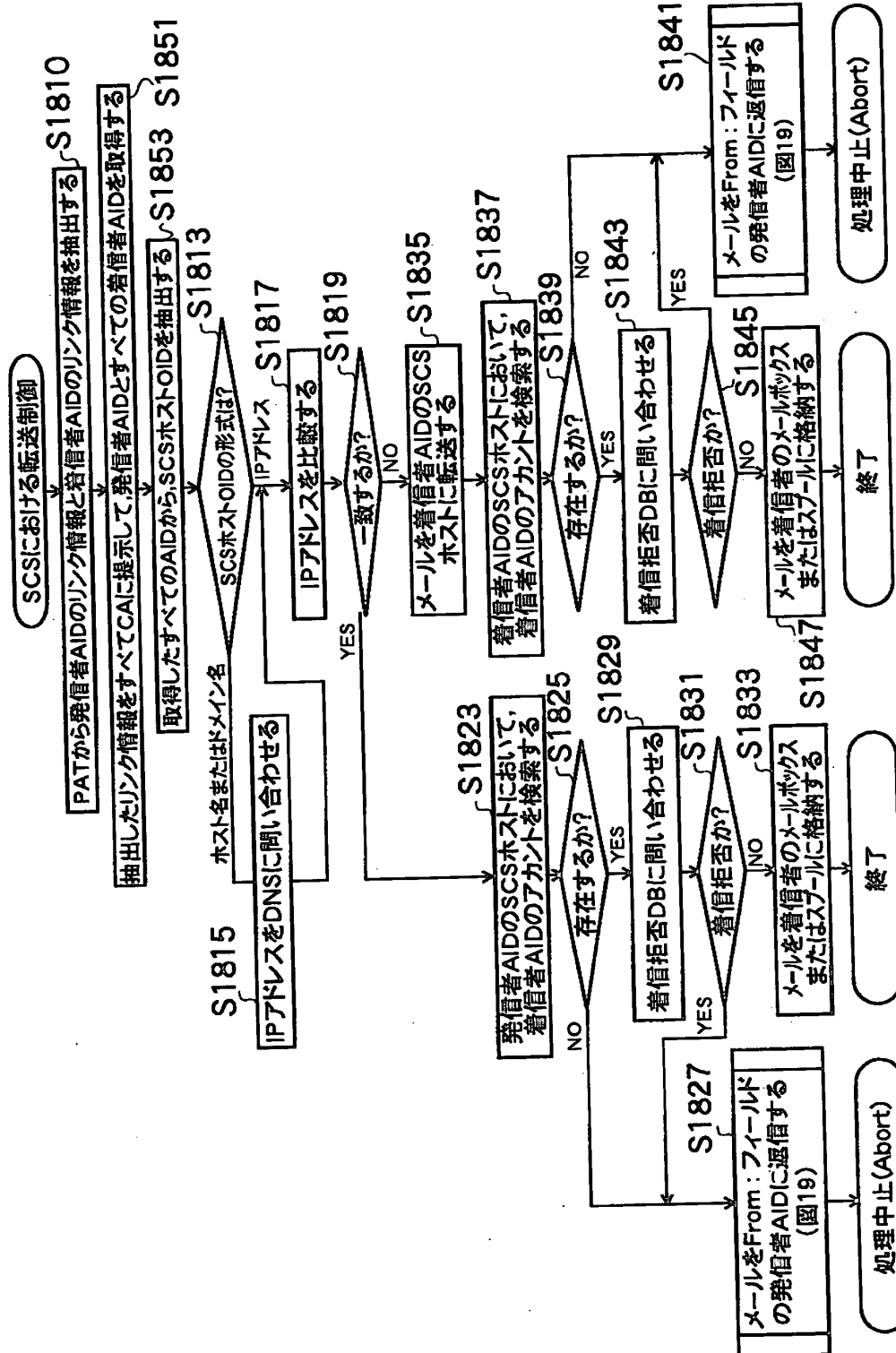


可変
検索者AIDが発信者の場合には、検索者AIDのメールクライアントが
発信者フラグをOに設定する。
逆に、登録者AIDが発信者の場合には、登録者AIDのメールクライアントが
発信者フラグをOに設定する。

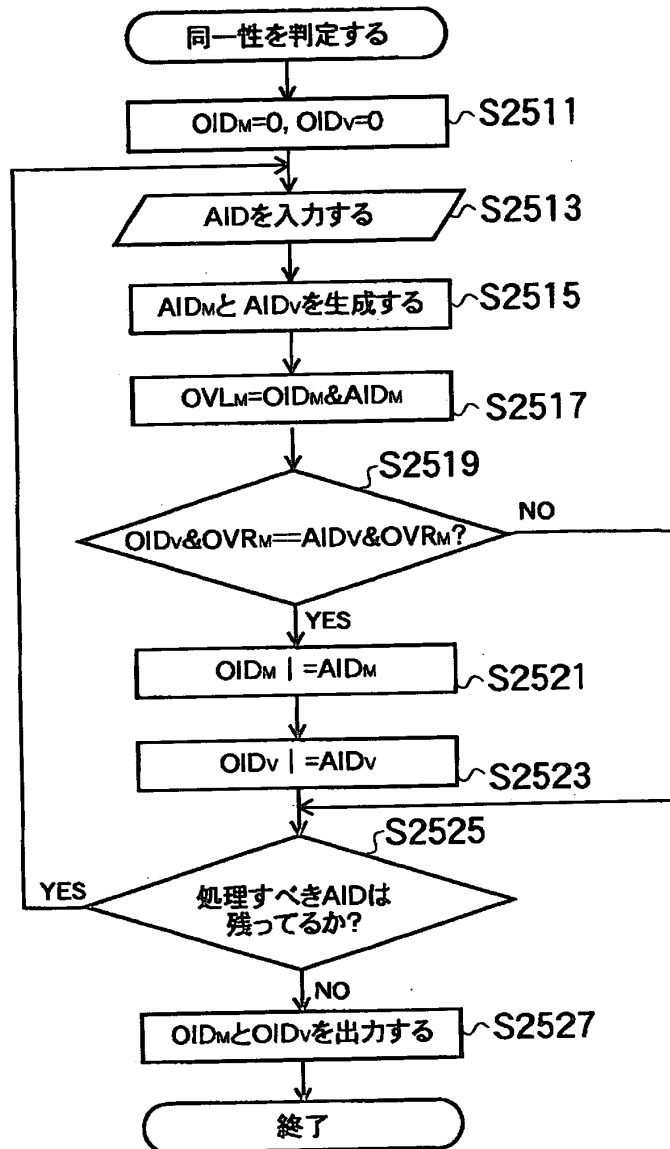
【図77】



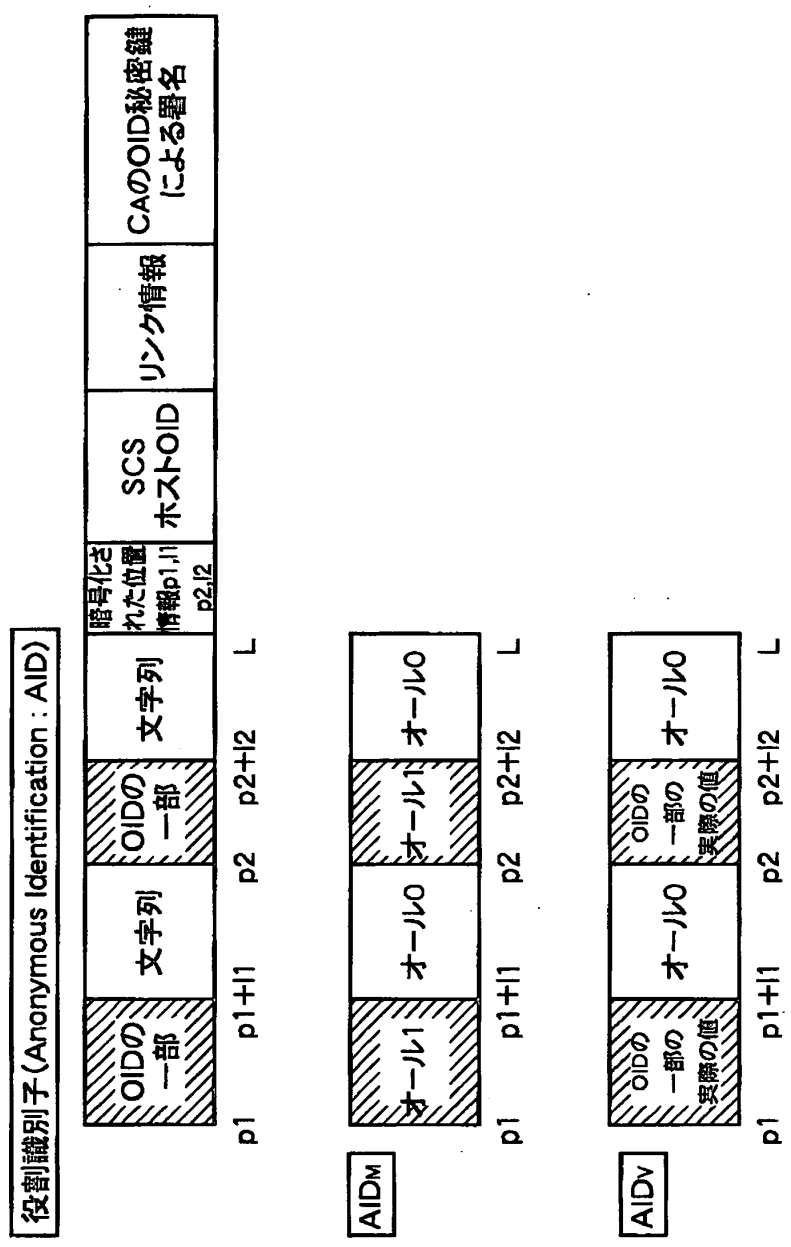
【图 7 8】



【図 79】

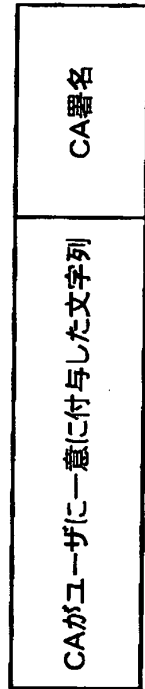


【図 80】

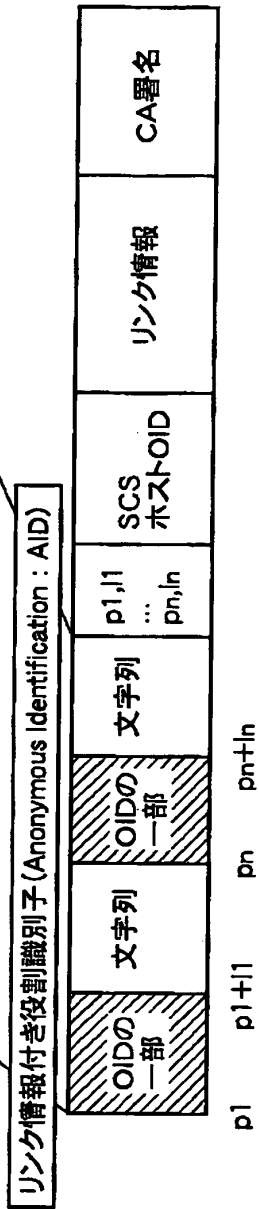


【図 81】

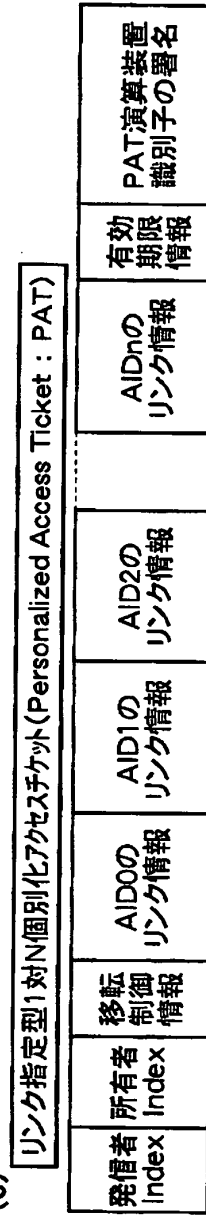
(a) 個人識別子 (Official Identification : OID)



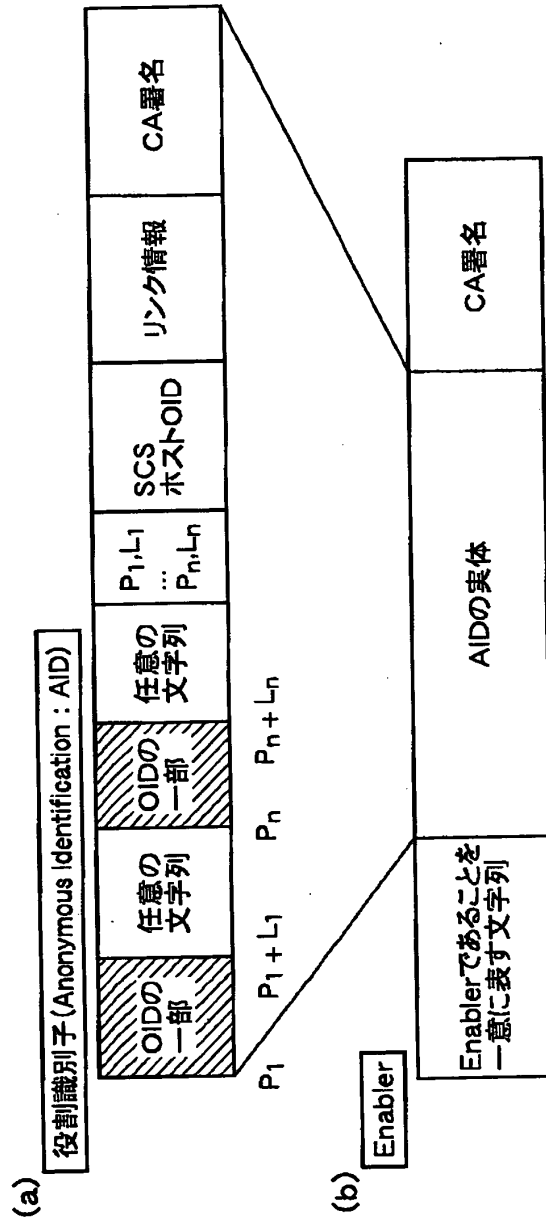
(b)



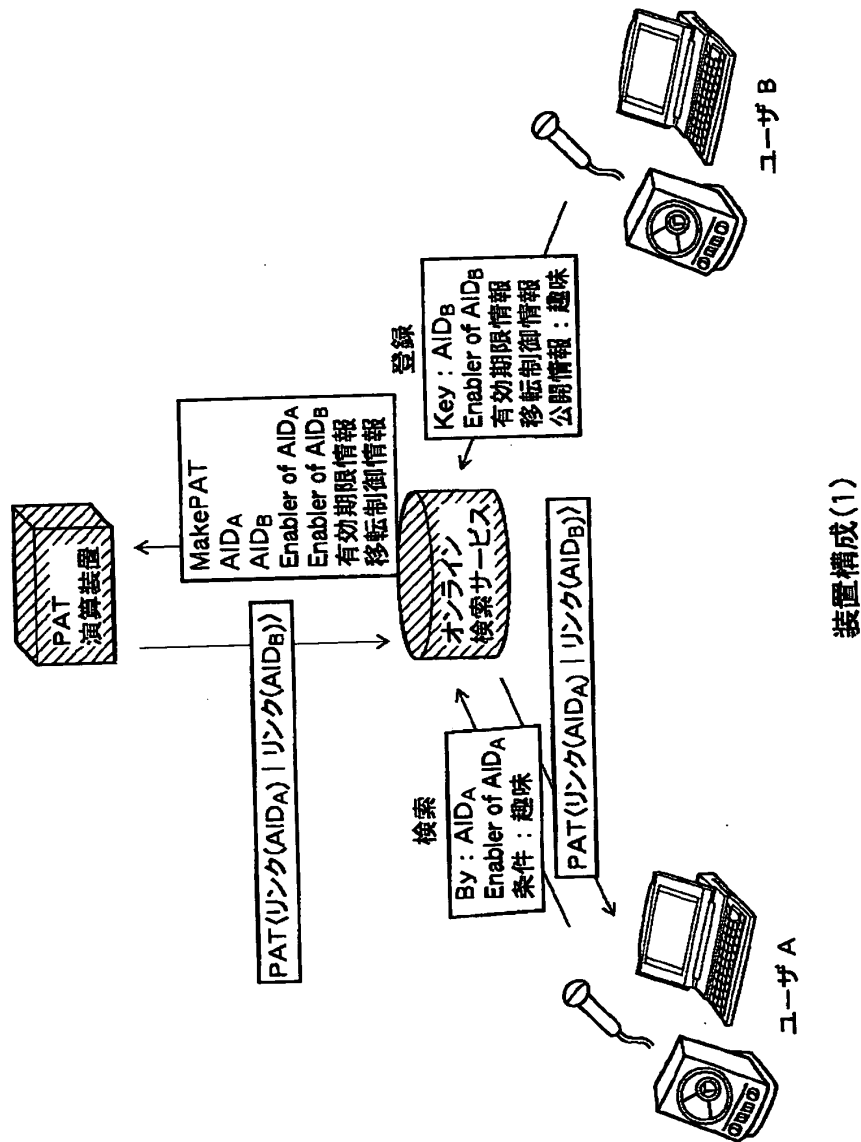
(c)



【図 82】

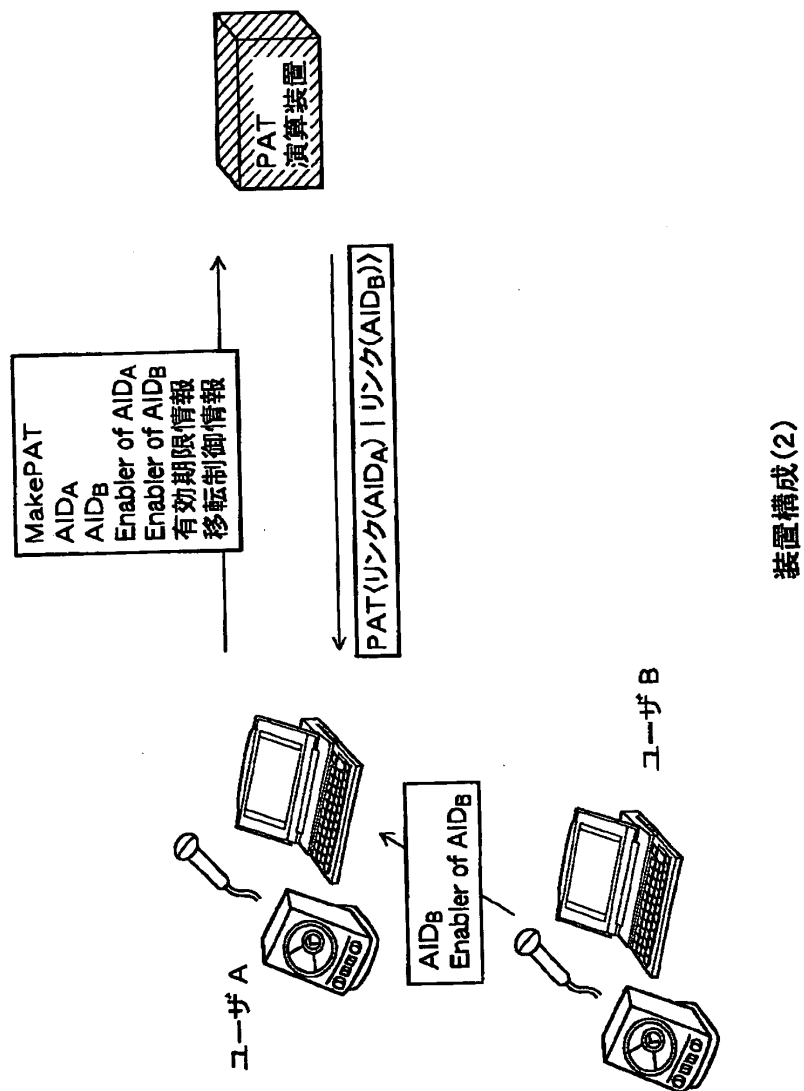


【図 83】

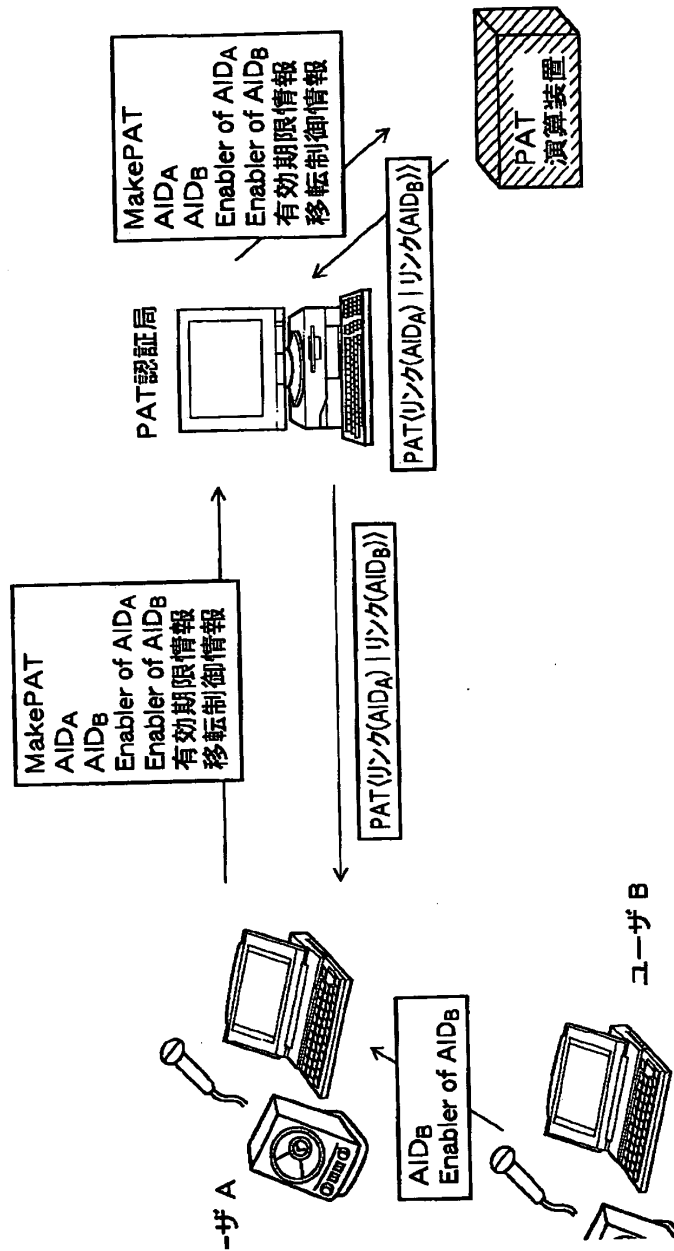


装置構成(1)

【図84】

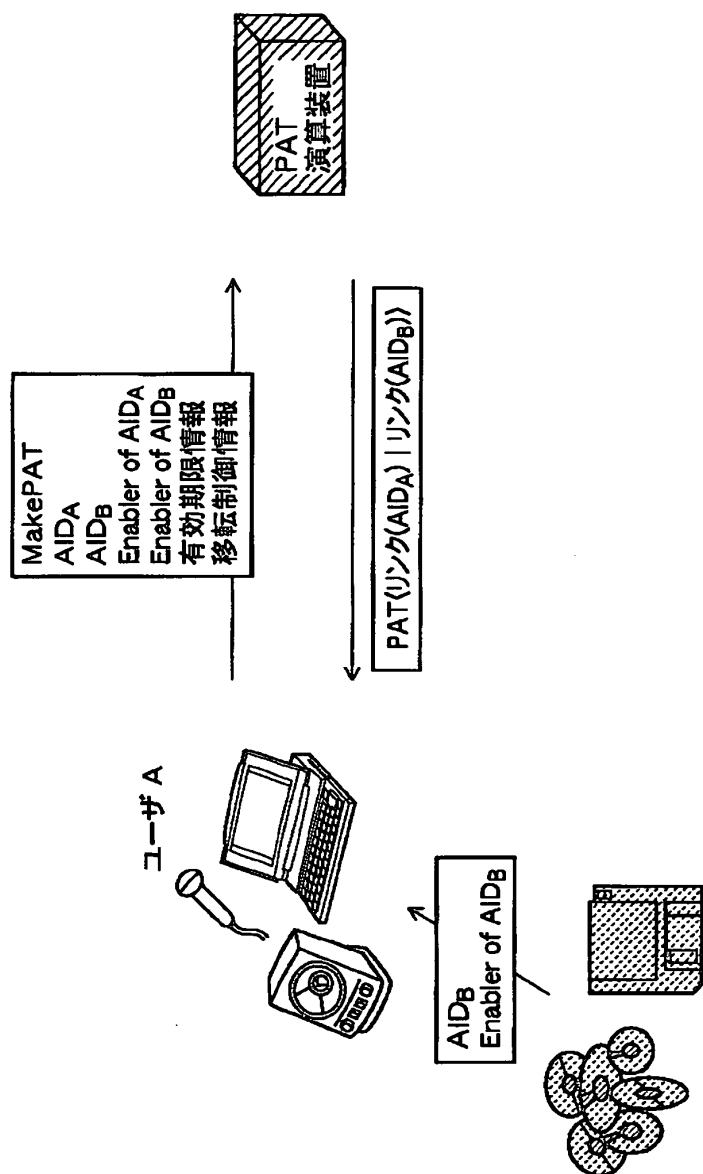


【図85】



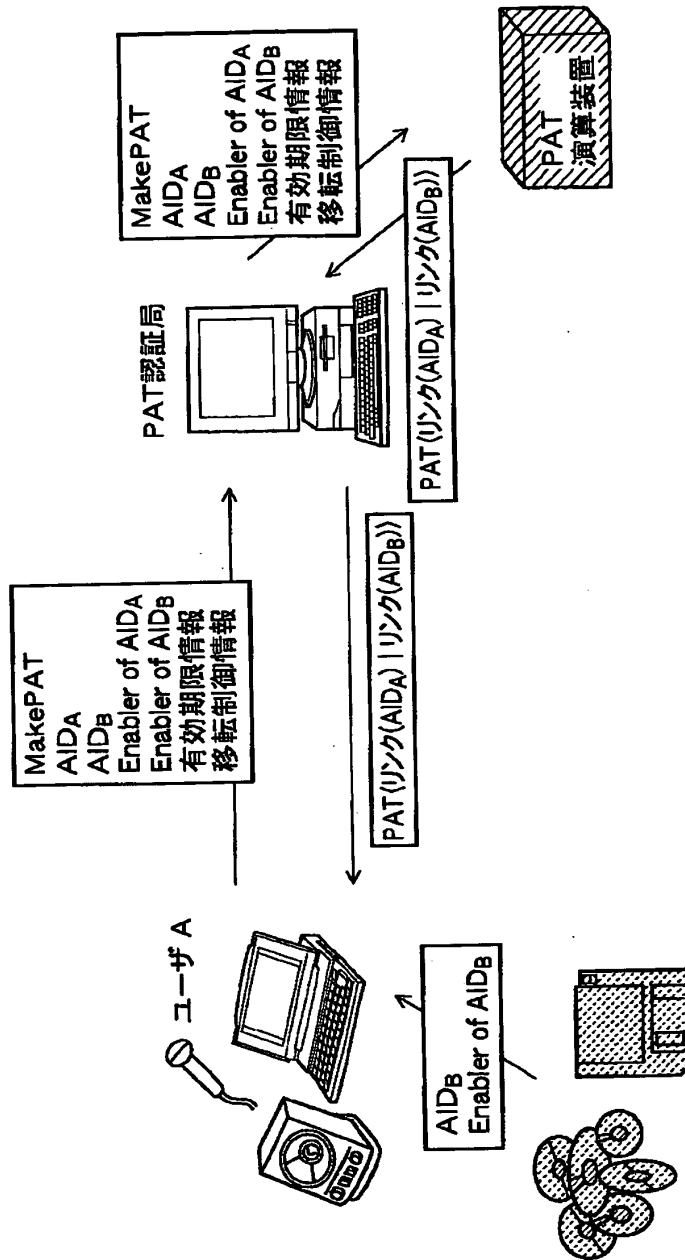
装置構成 (3)

【図 86】



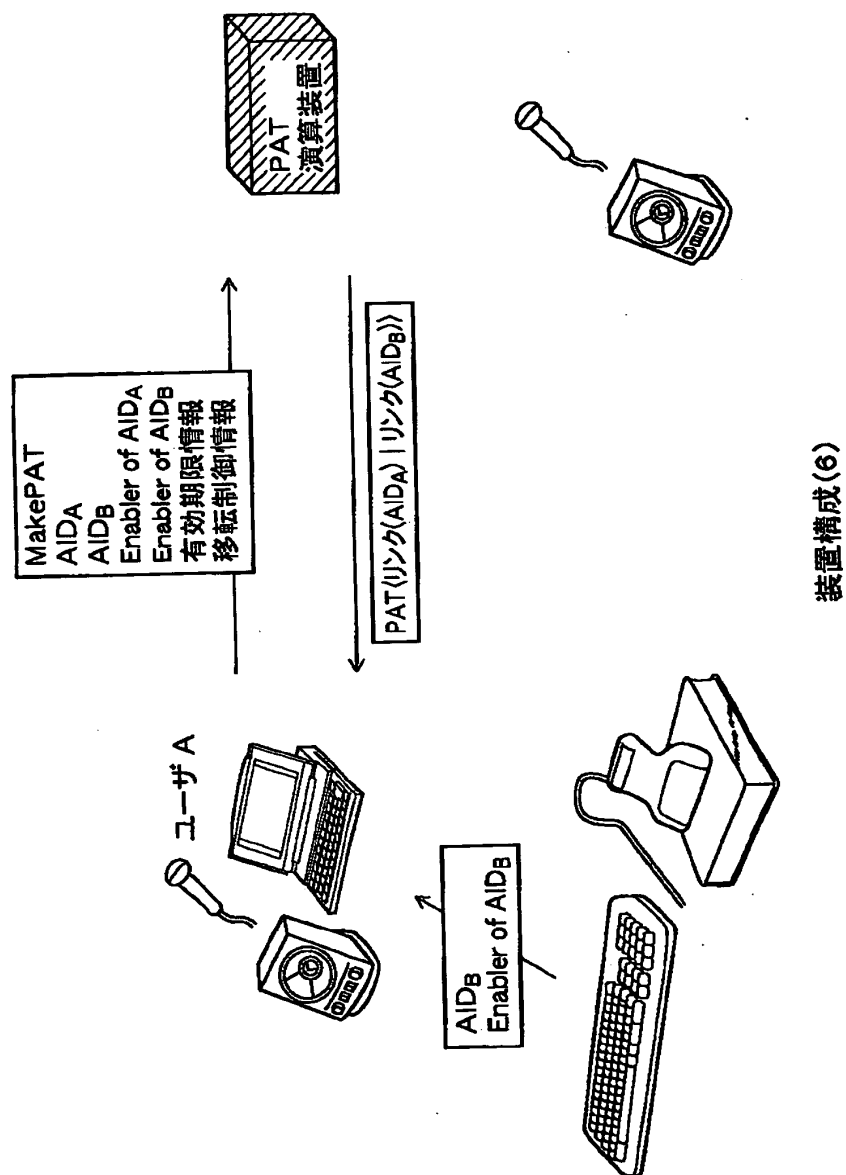
装置構成(4)

【図87】

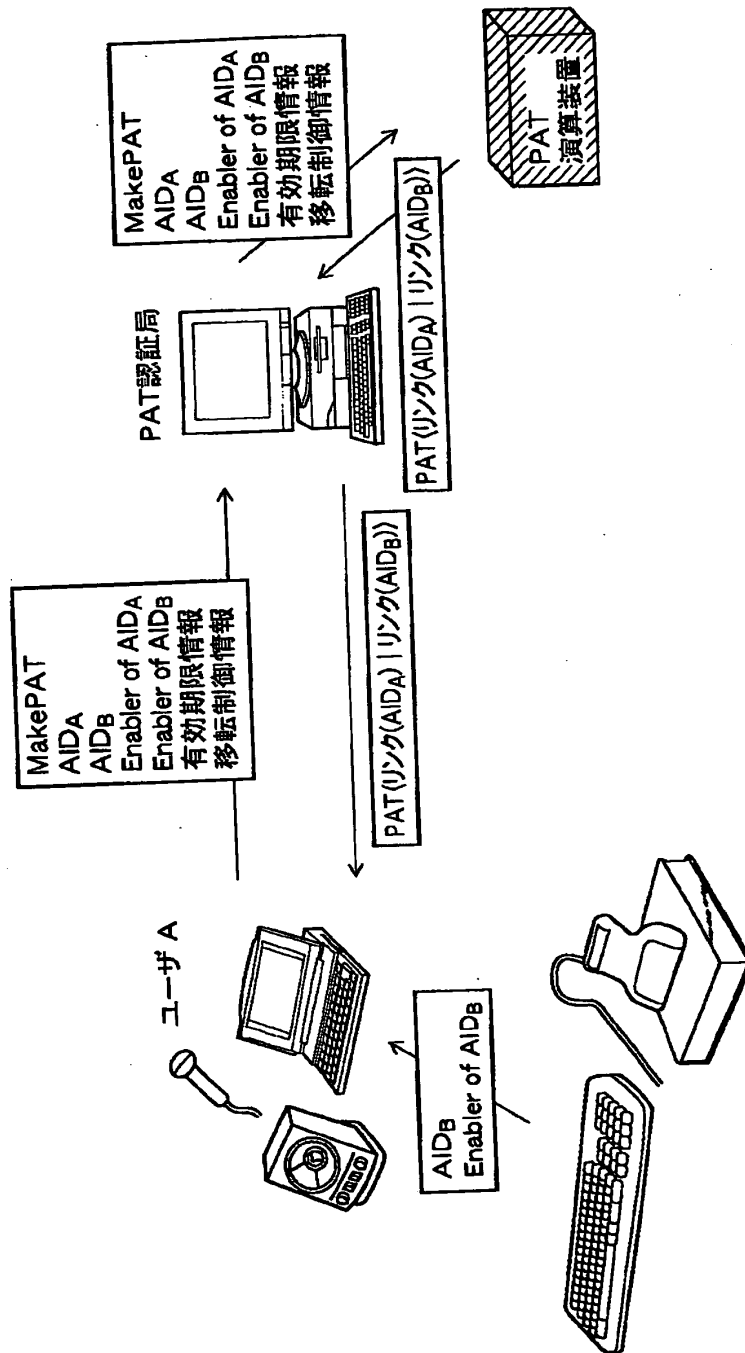


装置構成(5)

【図 88】

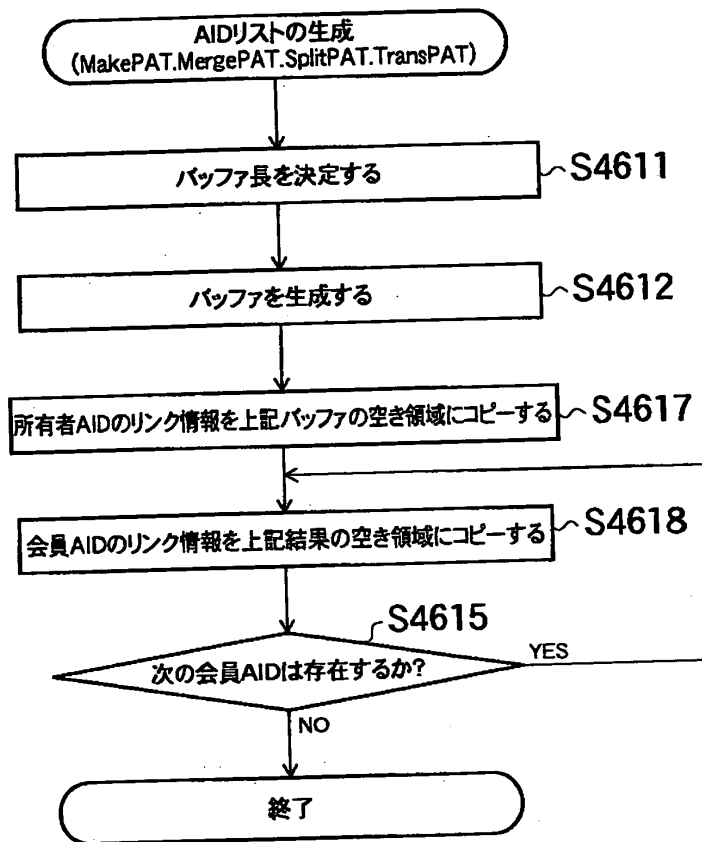


【図89】

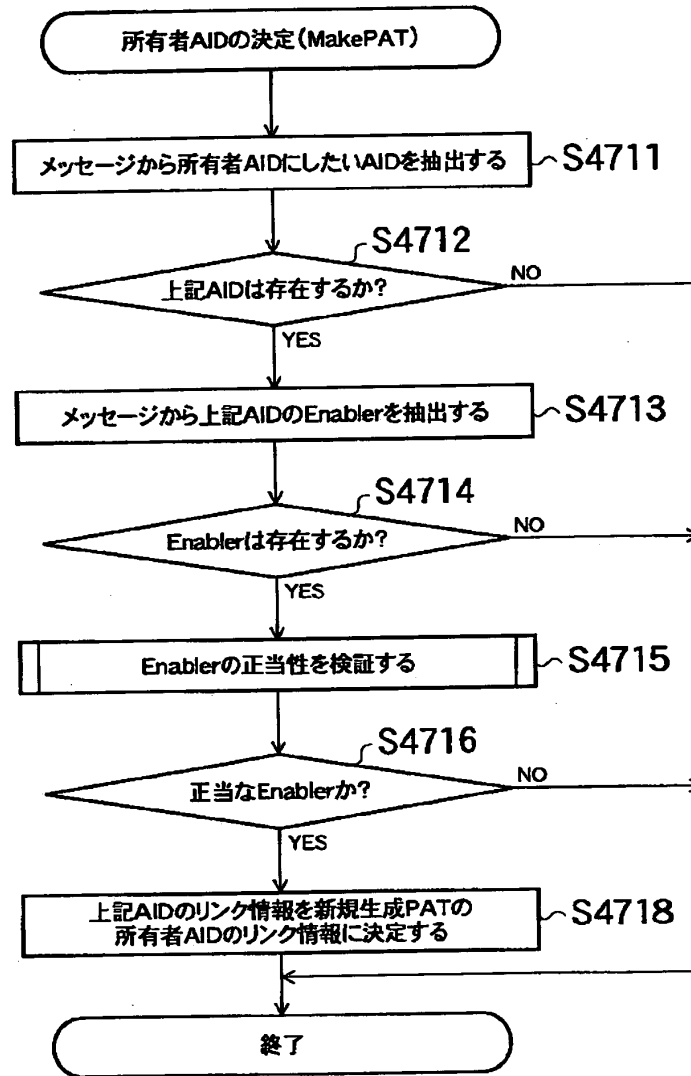


装置構成(7)

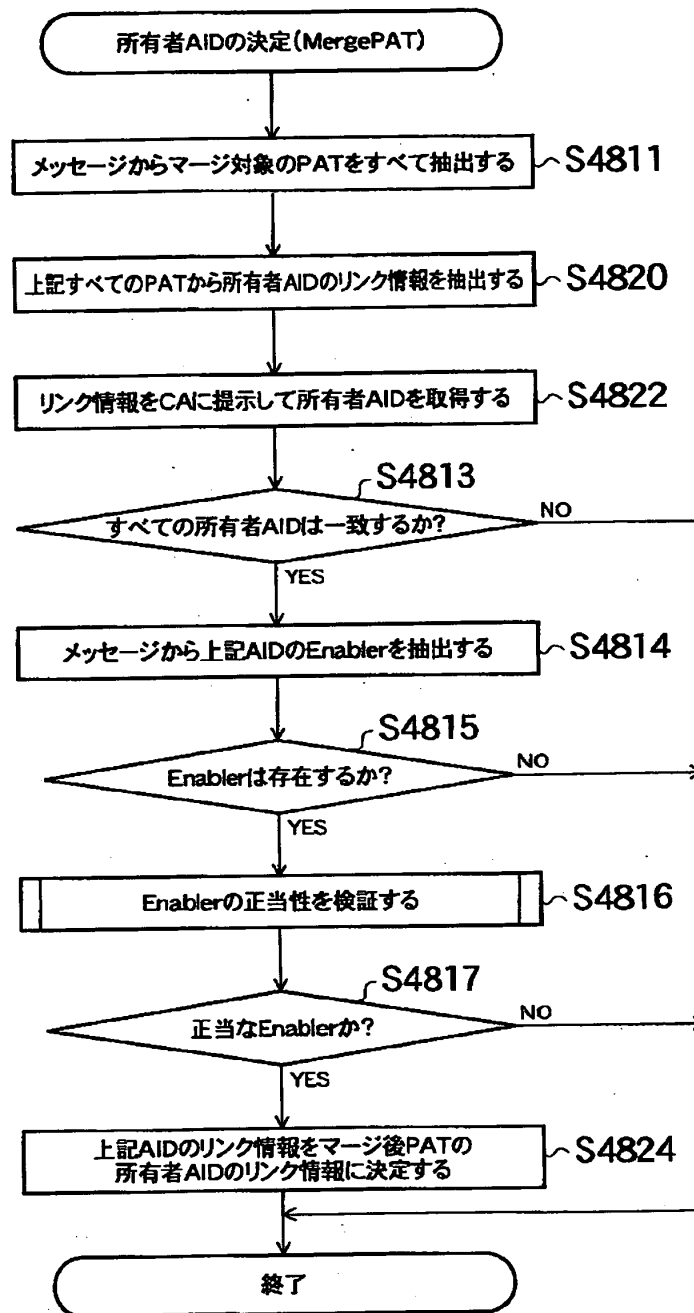
【図 90】



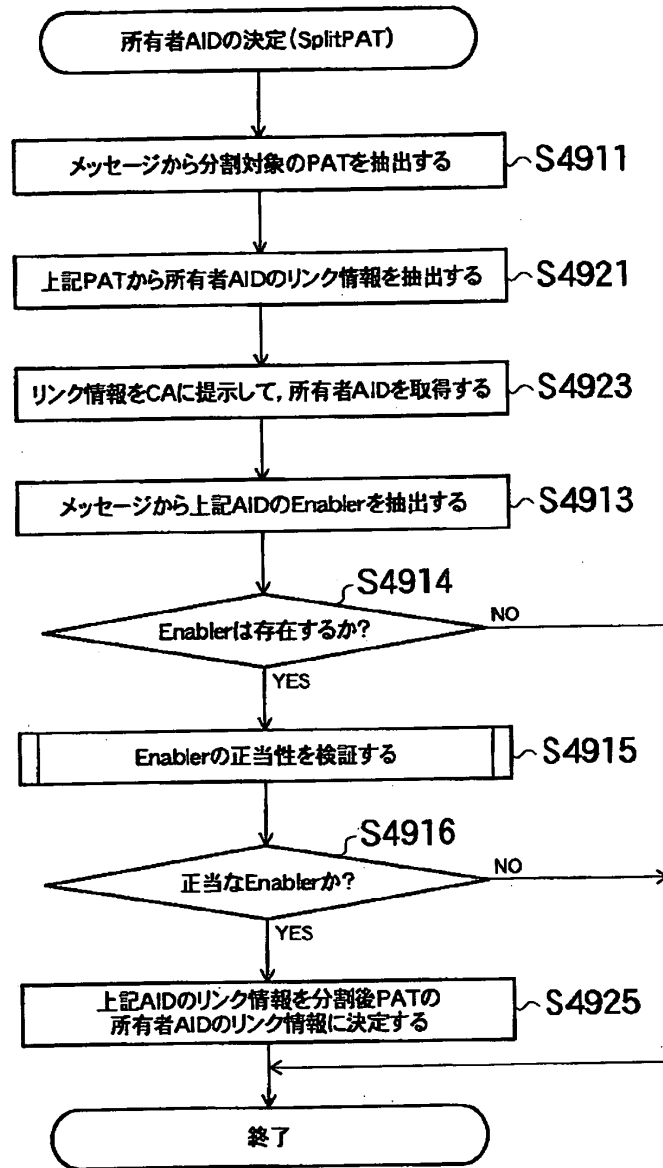
【図91】



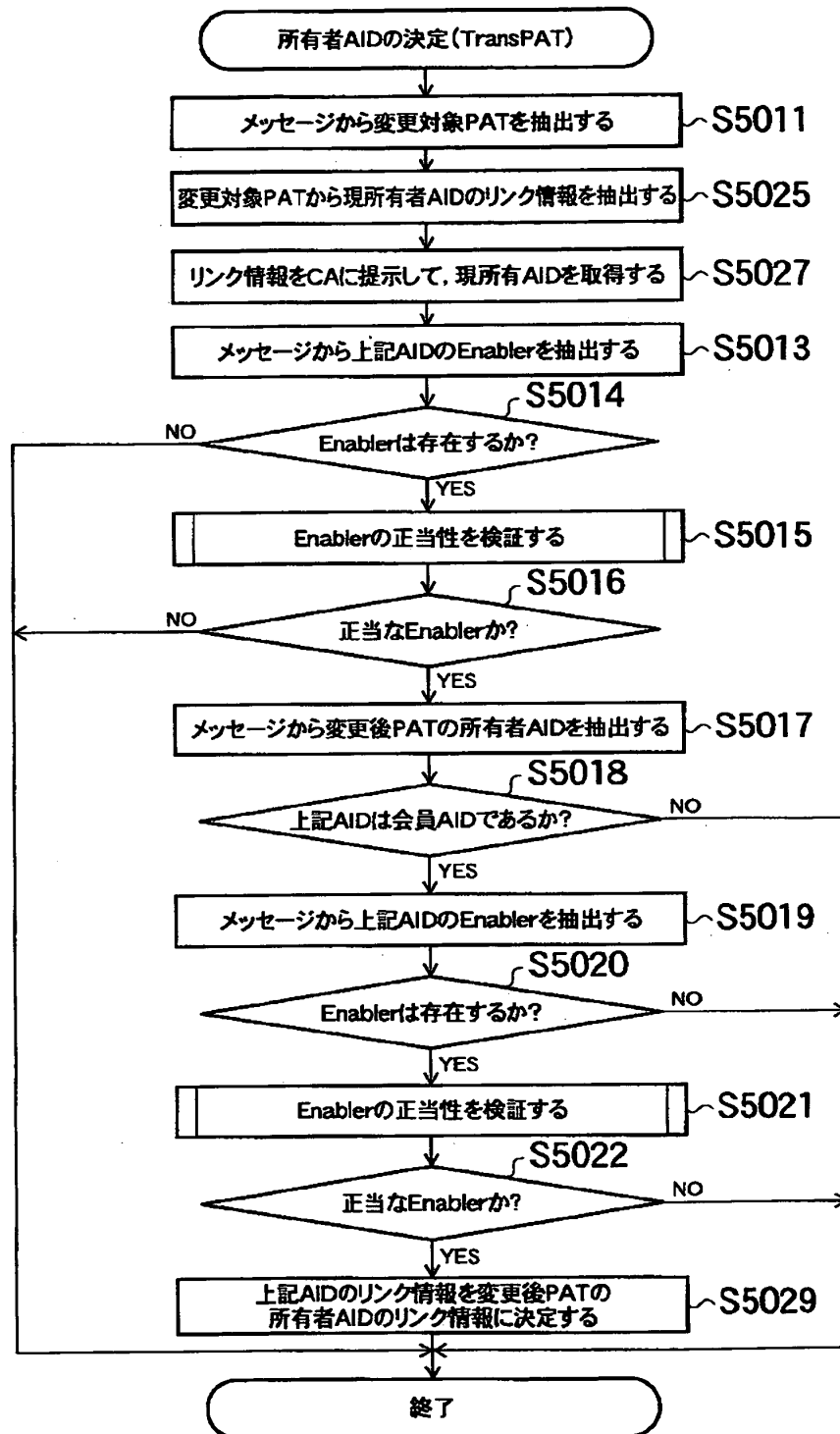
【図92】



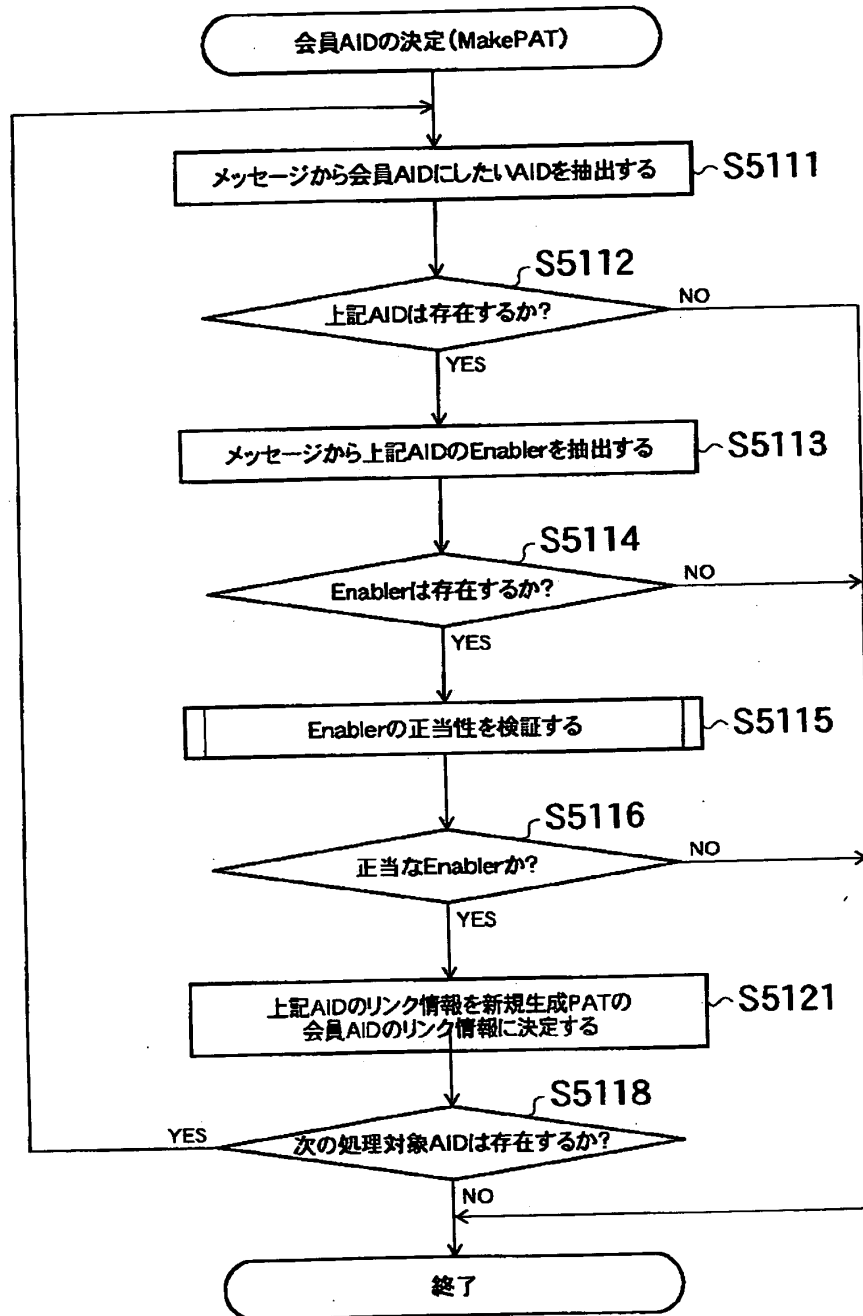
【図93】



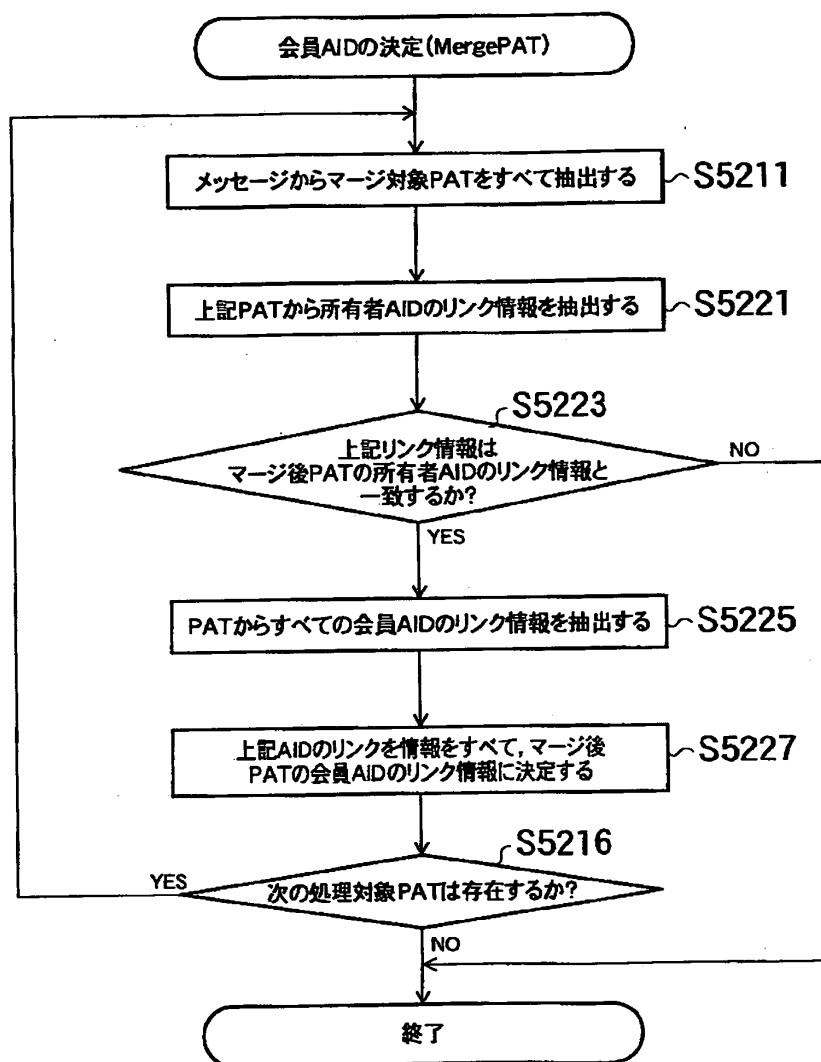
【図 94】



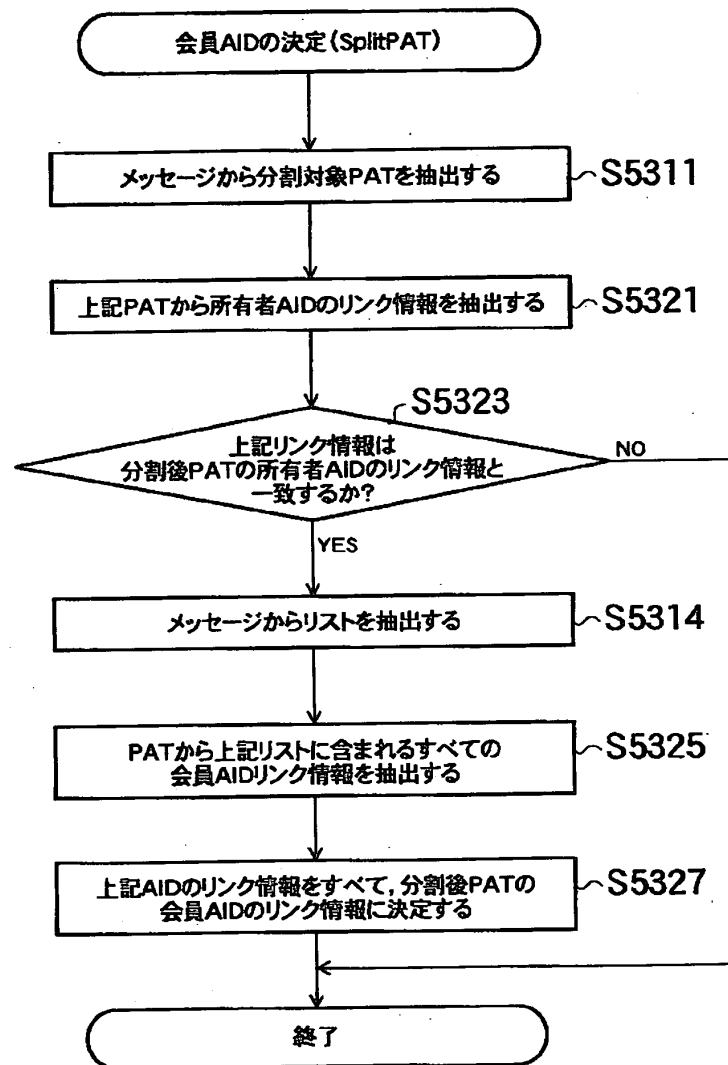
【図95】



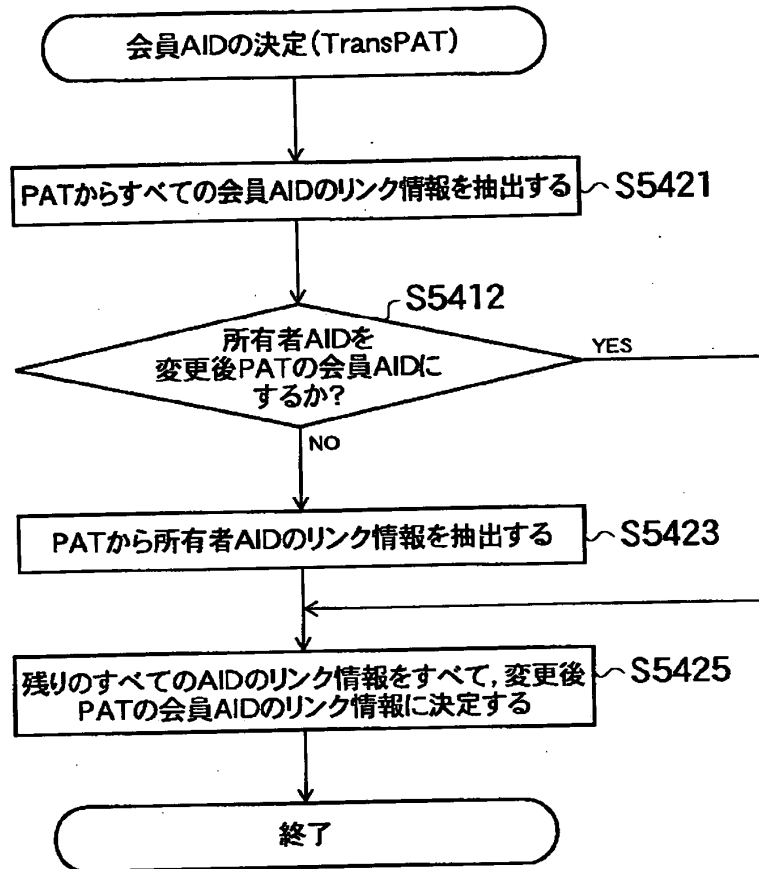
【図 96】



【図 97】



【図98】



【図99】

SplitPAT命令を含むメッセージ

SplitPAT
 分割対象PAT <リンク(所有者AID) | リンク(会員AID₁)、リンク(会員AID₂)...リンク(会員AID_n)>
 組み合わせ₁ (会員AID₁, 会員AID₃, 有効期限情報₁, 移転制御情報₁)
 組み合わせ₂ (会員AID₂, 会員AID₅, 有効期限情報₂, 移転制御情報₂)
 ...
 組み合わせ_n (会員AID_k, 会員AID_l, 有効期限情報_n, 移転制御情報_n)
 分割後PATの所有者AIDのEnabler

【図100】

TransPAT命令を含むメッセージ

TransPAT

所有権変更対象PAT <リンク(所有者AID) | リンク(会員AID₁),リンク(会員AID₂),...リンク(会員AID_n)>

所有者AIDのEnabler

所有権変更後PATの所有者AID 左記AIDのEnabler

有効期限情報

移転制御情報

【図101】

MergePAT命令を含むメッセージ

```
MergePAT
マージ対象PAT <リンク(所有者AID) | リンク(会員AID11) | リンク(会員AID12) ... リンク(会員AID1n)>
マージ対象PAT <リンク(所有者AID) | リンク(会員AID21) | リンク(会員AID22) ... リンク(会員AID2n)>
...
マージ対象PAT <リンク(所有者AID) | リンク(会員AIDm1) | リンク(会員AIDm2) ... リンク(会員AIDmn)>
マージ後PATの所有者AIDのEnabler
有効期限情報
移転制御情報
```

【書類名】 要約書

【要約】

【課題】 匿名性とセキュリティを確保すべく着信者の匿名性を保持しつつ発信者からの通信の接続を可能とする接続制御方法および通信網と接続制御プログラムおよびデータ構造を記録した記録媒体を提供する。

【解決手段】 ユーザに役割識別子を付与し、役割識別子とユーザに関する情報を閲覧可能に保持し、発信者は着信者を役割識別子で指定し、この指定に基づき発信者に発信者フラグ、移転制御フラグ、有効期限を含む個別化アクセスチケットを発行し、役割識別子と個別化アクセスチケットを用いて個別化アクセスチケットが有効期限内で正当であり、発信者役割識別子が個別化アクセスチケットに含まれ、着信者役割識別子が個別化アクセスチケットに含まれていることを検証し、検証結果がすべて正しい場合に発信者からの接続要求を通信網の物理的な接続制御方式に変換する接続制御を行う。

【選択図】 図1

【書類名】 職権訂正データ
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000004226

【住所又は居所】 東京都新宿区西新宿三丁目19番2号

【氏名又は名称】 日本電信電話株式会社

【代理人】 申請人

【識別番号】 100083806

【住所又は居所】 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル
9階 三好内外国特許事務所

【氏名又は名称】 三好 秀和

【選任した代理人】

【識別番号】 100068342

【住所又は居所】 東京都港区虎ノ門1丁目2番3号 虎ノ門第一ビル
9階 三好内外国特許事務所

【氏名又は名称】 三好 保男

特平10-315172

出願人履歴情報

識別番号

[000004226]

1. 変更年月日

1995年 9月21日

[変更理由]

住所変更

住 所

東京都新宿区西新宿三丁目19番2号

氏 名

日本電信電話株式会社